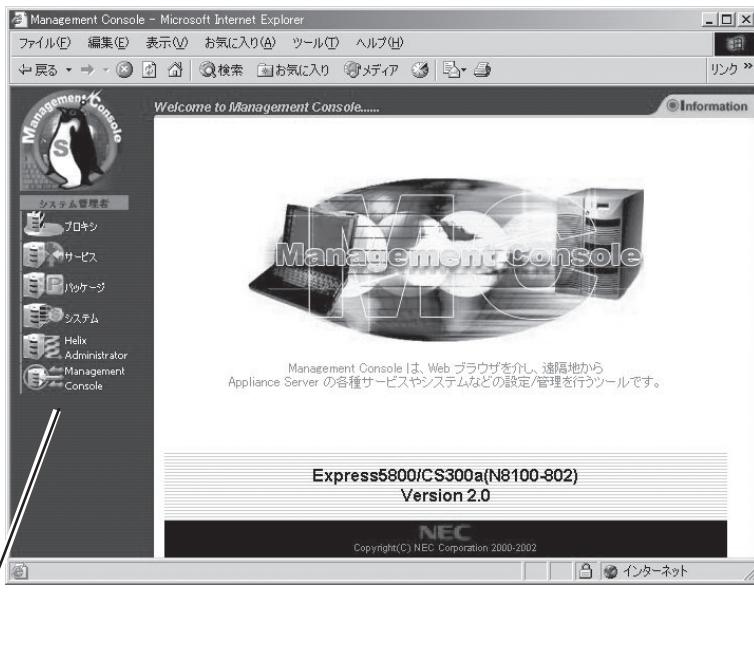
4 システムの管理

この章では、本装置で提供するサービスとWebベースの運用管理ツールである「Management Console」を利用した設定/管理について説明します。この「Management Console」からインターネットサービスに必要となるプロキシサーバを容易に管理することができます。

Management Consoleについて

ネットワーク上のクライアントマシンからWebブラウザを介して表示されるのが「Management Console」です。Management Consoleからシステムのさまざまな設定の変更や状態の確認ができます。

この章では、「管理者用」のManagement Consoleで利用できるさまざまなサービスの設定や確認、システムの操作方法を中心に説明します。

Management Console管理者用トップページ

ブラウザ上から項目(アイコン)をクリックすると、それぞれの設定画面に移動することができる。

【Management Consoleの画面構成】

■ システム管理者用トップページ

- プロキシ
- サービス
- パッケージ
- システム
- Helix Administrator
- Management Console*

* 本書では説明していません。Management Consoleのオンラインヘルプを参照して操作してください。

Management Consoleのセキュリティモード

Management Consoleでは、日常的な運用管理のセキュリティを確保するためManagement Consoleに2つのセキュリティモードをサポートしています。

- **レベル1（パスワード）**

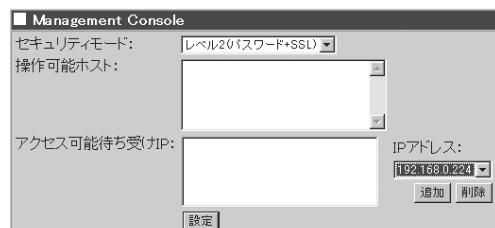
  パスワード認証による利用者チェックを行います。ただし、パスワードや設定情報は暗号化されません。

- **レベル2（パスワード + SSL）**

  パスワード認証に加えて、パスワードや設定情報をSSL（Secure Soket layer）で暗号化して送受信します。自己署名証明書を用いていますので、ブラウザでアクセスする際に警告ダイアログボックスが表示されますが、[はい]などをクリックしてください。

デフォルトの設定では、「レベル2」に設定されています。セキュリティレベルを変更する場合は、Management Console画面の［Management Console]アイコンをクリックして設定を変更してください。また、同画面で操作可能ホストを設定することにより、さらに高いレベルのセキュリティを保つことができます。

アクセス可能待ち受けIP

本製品に割り当てられているIPアドレスの中から、Management Consoleのアクセスを許可するIPを指定します。例えばローカルIPとグローバルIPが割り当てられている場合、ローカルIPのみでアクセスを許可し、グローバルIPはアクセスを拒否する事で、本製品のセキュリティを高める事が可能です。リストボックスが空の場合は、すべてのIPでアクセスを受け付けます。

Management Consoleへのアクセス方法

システム管理者は、Management Consoleを利用することにより、クライアント側のブラウザからネットワークを介してあらゆるサービスを簡単な操作で一元的に管理することができます。以下に各セキュリティモードにおけるアクセス手順を示します。

重要

- **Management Consoleへのアクセスには、プロキシを経由させないでください。**
- **インターネット側からManagement Consoleにアクセスする場合は、レベル2に設定してください。**
- **レベル2では、HTTPSプロトコル、ポート番号50453を使用します。**
- **Management Consoleへアクセスする場合にはブラウザのキャッシュ機能を使用しないようにしてください。**

レベル1の場合

1. クライアント側のブラウザを起動する。
2. URL入力欄に「http://<本装置に割り当てたIPアドレスまたはFQDN>:50090/」と入力する。
3. Management Console」画面で、[システム管理者ログイン]をクリックする。
4. ユーザー名とパスワードの入力を要求されたら、ユーザー名には「admin」、パスワードにはセットアップ時に指定した管理者パスワードを入力する。

レベル2の場合

1. クライアント側のブラウザを起動する。
2. URL入力欄に「https://<本装置に割り当てたIPアドレスまたはFQDN>:50453/」と入力する。
3. 警告ダイアログボックスが表示されたら、[はい]などをクリックして進む。
4. [Management Console]画面で、[管理者用]をクリックする。
5. ユーザー名とパスワードの入力を要求されたら、ユーザー名には「admin」、パスワードにはセットアップ時に指定した管理者パスワードを入力する。

Management Consoleにログインできたら、Management Console管理者用のトップページが表示されます。

プロキシ

頻繁にアクセスするページをキャッシングすることにより、次回、同じページにアクセスした際に、ブラウザの表示時間を短縮します。
管理者は、Management Consoleから、有害なWebサイトなどへのアクセスの制限、不正なアクセスの制限などを設定することができます。
また、頻繁に参照されるWebページをシステムに自動的にダウンロードさせ、システム内に格納しておくための設定もできます。
これらの設定により、効率的なインターネットへのアクセスを実現します。

【プロキシサーバの状態】

- プロキシサーバの状態表示、および起動/再起動設定

  プロキシサーバの起動状態を表示します。

- スケジュールダウンロードの状態表示、および一時停止/起動設定

  コンテンツを定期的にダウンロードしてキャッシュに格納するスケジュールダウンロードの状態を表示します。

【プロキシサーバの設定】

- 基本設定

  ブラウザからの要求を受け付けるIPアドレスやポート番号など、プロキシを動作させるための基本的な設定をサーバ種別に応じて設定します。

- 親プロキシ設定

  親プロキシの指定と、親プロキシの選択方法を設定します。

- 隣接プロキシ

  隣接プロキシを指定し、隣接プロキシの問い合わせ方法の設定をします。

- 詳細設定

  最大キャッシュサイズなどの詳細な設定をします。

- アクセス制御

  アクセス制御に関する設定をします。

- スケジュールダウンロード

  頻繁に参照されるページをあらかじめ指定時刻にダウンロードし、キャッシュに入れておくための設定をします。

- 認証設定

  LDAP、RADIUSサーバに対する認証のための設定をします。

- バイパス設定

  透過型プロキシとして動作する際の、静的バイパス・動的バイパスの設定を行います。

【フィルター設定】

- フィルター選択

  使用するフィルタリングソフトを選択します。選択されたフィルタリングソフトに応じて下記の設定画面へのリンクが表示されます。

- SmartFilter設定

  SmartFilterを使用するための設定をします。

- Interscan設定

  Interscanを使用するための設定をします。

プロキシサーバの状態

[プロシキ]画面の[プロシキサーバの状態]で設定できる項目について説明します。

プロキシサーバ

プロキシサーバの状態を表示します。[再起動]をクリックするとプロキシサーバの再起動を行います(システムは再起動しません)。

スケジュールダウンロード

コンテンツを定期的にダウンロードしてキャッシュに格納するスケジュールダウンロードの状態を表示します。スケジュールダウンロードの使用を止める場合には、[一時停止]をクリックしてください。スケジュールダウンロードの再開は[起動]をクリックします。

プロキシサーバの設定

[プロシキ]画面の[プロシキサーバの設定]で設定できる項目について説明します。

基本設定(Forwardプロキシ)

[プロキシ]画面の[基本設定]でプロキシサーバの基本的な動作設定ができます。[基本設定]画面では、以下の項目の設定ができます。

● **サーバ種別設定**

プロキシサーバの動作種別を、[Forward]、[Forward(透過型L4スイッチ)]、[Forward(透過型WCCP)]、[Reverse]の4つから選択します。

[Reverse]を選択した場合は、リバースプロキシの設定ページが表示されます。

● **キャッシュサーバ設定**

キャッシュサーバのIPアドレスと、HTTPの要求を受け付けるポート番号を指定します。登録されているIPアドレスとポート番号の組は、リストボックスに表示されます。[追加]、[編集]、[削除]で、設定を行います。

- **登録できるIPアドレスとポート番号の組は最大16個です。**
- **[キャッシュサーバIPアドレス]で選択できるIPアドレスは、[システム]−[ネットワーク]-[インターフェイス]画面で登録したIPアドレスのみが表示されます。**

● **ICPポート番号設定**

システムがICP要求を受け付けるポート番号を指定します。通常は3130を指定します。ICP要求を受け付けたくない場合には「ICP要求を受け付けない」を指定してください。

システムがICPサーバとして動作する場合、システムのIPアドレスは一種類となります(複数に対応していません)。隣接プロキシ側に設定するシステムのIPアドレスはシステムのネットワークのインターフェイス画面で一番上に登録したIPアドレスを適用してください。

- **WCCP設定**

  ルータアドレスで、WCCPルータのIPアドレスを指定します。登録されているWCCPルータのIPアドレスはリストボックスに表示されます。[追加]、[編集]、[削除]で設定します。

  － キャッシュサーバIPアドレス

    WCCPルータからパケットを転送するキャッシュサーバのIPアドレスを指定します。

  － バージョン

    WCCPのバージョンを指定します。指定できるバージョンは[1]か[2]です。

  － マルチキャストIP

    WCCPルータがマルチキャストIPを使用するかどうかを指定します。指定できるIPアドレスの範囲は、224.0.0.0-239.255.255.255になります。マルチキャストIP使用時はルータアドレスの設定は無効になります。

  － パスワード

    認証を行うためのパスワードを指定します。

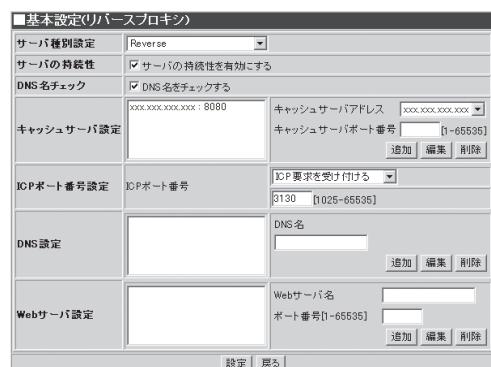
  － HASH方法

    HASH方法を指定します。

重要

- **WCCP設定は、サーバ種別で[Forward(透過型WCCP)]を選択した時のみ有効になります。**
- **[設定]をクリックしないと、システムに反映されません。**
- **設定項目の詳細は、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

基本設定(Reverseプロキシ)

[プロキシ]画面の[基本設定]でサーバ種別設定を「Reverse」と選ぶことによって表示される画面です。この画面では、システムをリバースモードで運用する際の設定ができます(システムをリバースモードで運用するには DNSサーバとの連携が必須です)。

- **サーバ種別設定**

  リバースモードで動作するため、「Reverse」と言う文字が表示されています。

- **サーバの持続性**

複数Webサーバの負荷を軽減するためシステムを導入する場合、クライアントIPアドレスによって接続するWebサーバを一意に限定したい場合に有効にしてください。このチェックをONにすることによりクライアントは複数あるWebサーバの内常に特定のWebサーバにアクセスすることが可能となります(注：システムに直接接続してきているクライアントのIPアドレスによって持続性を確保しているため、接続ルートが異なると持続性が確保されません)。

- **DNS名チェック**

システムが受け付けた要求に示されているWebサーバのホスト名と下記DNS設定にて設定したDNS名(ホスト名)が同一となっているかチェックしたい場合に有効にしてください。有効にした場合にどのDNS名とも同一でないホスト名の要求は拒否されます。

> **重要** HTTPSの場合はチェックされません。

- **キャッシュサーバ設定**

システムのHTTP要求を受け付けるIPアドレスとポート番号を設定します。

- **DNS設定**

Internetに公開するWebサーバのホスト名を設定してください。また、システムは 一つのIPアドレスに対して複数のホスト名を持つことができます。別々のコンテンツを持つ2つのWebサーバのホスト名をシステムのIPアドレスに解決されるようにDNSサーバに設定してください。システムは ホスト名を見分けて別々に処理することができます。

- **Webサーバ設定**

実際のWebサーバのIPアドレスとポート番号を指定してください。また、システムは 一つのDNS名に対して複数のWebサーバを設定できます(このような構成とした場合 設定された複数のWebサーバは同一のコンテンツを提供する必要があります)。

> **重要**
> - キャッシュサーバを登録、変更する場合には 必ず、[追加]、[編集]をクリックしてください。DNS設定やWebサーバ設定についても同様です。
> - [設定]をクリックしないと、システムに反映されません。
> - ReverseHTTPSとして運用される場合には、DNS名は1つしか設定しないでください。
> - HTTPSのポート番号は、443で固定です。
> - リバースプロキシが対応するプロトコルはHTTPとHTTPSです。

親プロキシ設定

階層構造を形成する場合に親プロキシを設定することができます。

- **ホスト名**

  親プロキシのホスト名 又は IPアドレスを設定してください。隣接プロキシに設定してあるホスト名およびIPアドレスは指定できません。

- **HTTPポート番号**

  親プロキシのHTTP要求待ち受けポート番号を指定してください。

- **連携サーバのコンテンツをキャッシュ**

  親プロキシを経由して取得したコンテンツをキャッシュして欲しくない場合に「しない」を設定してください。

- **ユーザ名/パスワード/パスワード確認**

  親プロキシが認証機能を有している場合、ユーザー名、パスワードの指定を行います。親プロキシが認証を必要とする場合はユーザー名、パスワードの指定は必須です。親プロキシに接続する際に指定したユーザー名とパスワードでアクセスします。親プロキシが認証を必要としない場合は、設定する必要はありません。

- **プロキシ選択方式**

  複数の親プロキシを設定した場合に、その中からどの親プロキシを選ぶかといった選択方式を設定できます。

  ー　アクセス制御を使用

  条件式を満たした場合に現在選択されている 親プロキシに接続する方式(条件式の具体例はManagemant Consoleのヘルプを参照してください)。

  ー　ROUND-ROBINを使用

  複数の親プロキシを順番に選択する方式です。その際、現在選択されている親プロキシが選択される頻度を重み付けとして設定できます(数字が大きいほど頻度が高くなります)。

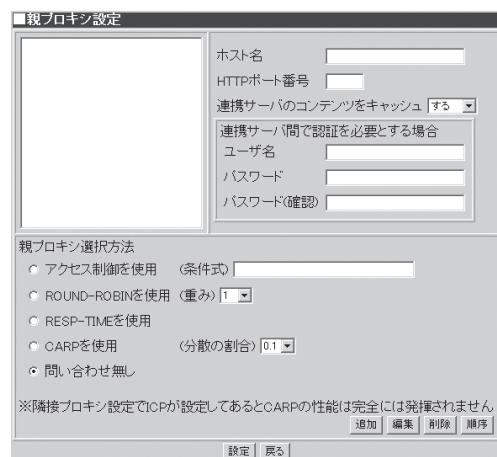
  ー　RESP-TIMEを使用

  応答速度の速い親プロキシが優先的に選択される方式。

  ー　CARPを使用

  URLごとに接続先の親プロキシを一意に選択するプロトコル「CARP」を利用する方式。 現在選択されている親プロキシが選択される割合を指定できます(割合の合計が1.0になるように設定してください)。

  ー　問い合わせなし

  親プロキシが単一の場合はこの設定にしてください。

親プロキシの選択方法にアクセス制御を使用を選んだ場合、条件式は、親プロキシの一覧の上位にあるものからチェックされます。

- **親プロキシを登録、変更する場合には必ず、[追加]、[編集]をクリックしてください。**
- **[設定]をクリックしないと、システムに反映されません。**

隣接プロキシ設定

階層構造を形成する場合にシステムの隣接プロキシを設定することができます。

- **ホスト名**

  隣接プロキシのホスト名 又は IPアドレス を設定してください。親プロキシに設定してあるホスト名およびIPアドレスは指定できません。

- **HTTPポート番号**

  隣接プロキシのHTTP要求待ち受けポート番号を指定してください。

- **ICPポート番号**

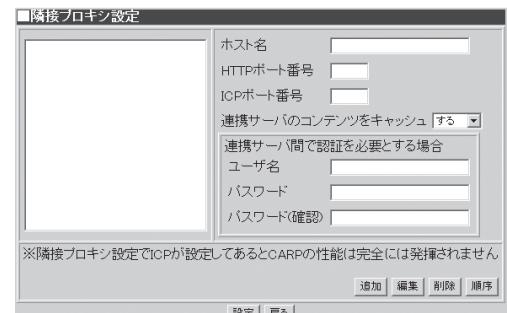
  隣接プロキシとICP要求待ち受けポートを指定してください。システムは隣接プロキシと連携する際にICPを利用します。

- **連携サーバのコンテンツをキャッシュ**

  隣接プロキシを経由して取得したコンテンツをキャッシュしたくない場合に「しない」を選択してください。

- **ユーザ名/パスワード/パスワード確認**

  隣接プロキシが認証機能を有している場合、ユーザー名、パスワードの指定を行います。隣接プロキシが認証を必要とする場合はユーザー名、パスワードの指定は必須です。隣接プロキシに接続する際にこのユーザー名とパスワードでアクセスします。隣接プロキシが認証を必要としない場合は、設定する必要はありません。

[重要] 隣接プロキシを設定すると、指定した隣接サーバの設定によっては、web閲覧の際にページや画像が正しく表示されない場合があります。指定した隣接サーバの設定を確認し、設定し直すか、ここでの設定を削除してください(7章の「トラブルシューティング」も併せて参照してください)。

詳細設定

[プロキシ]画面の[詳細設定]でプロキシサーバとしての詳細な動作設定ができます。
[詳細設定]画面では、以下の項目の設定ができます。

■ 詳細設定

項目	設定値
最大キャッシュサイズ	16 MB
Webサーバ接続最大待ち時間	120 秒
Read要求最大待ち時間	15 分
クライアント接続維持時間	300 秒
最大クライアント接続維持時間	1 日
クライアントIPの通知	しない
リクエストボディサイズの上限値	1 MB
レスポンスサイズの上限値	1 GB
DNSリトライ間隔	3 秒
DNSリトライ数	4 回
FTPのPASVモード	有効にする
FTPのパスワード	guest@
Viaヘッダ	1.1 test.nig.nes.nec
キャッシュログ出力	OFF
キャッシュ有効時間	6 時間

デフォルト値に戻す

設定 戻る

● **最大キャッシュサイズ**

この設定サイズよりも大きなデータはディスクに保存されません。0KB～999MBまで指定できます。0が指定されると制限無しとなります。デフォルトは[16MB]です。

● **Webサーバ接続最大待ち時間**

Webサーバとの接続タイムアウト時間を指定します。30秒～99日まで指定できます。デフォルトは[120秒]です。

● **Read要求最大待ち時間**

Webサーバへの要求に対して応答待ちをする時間を指定します。30秒～99日まで指定できます。デフォルトは[15分]です。

● **クライアント接続維持時間**

クライアントからの接続を維持する最大無応答時間を指定します。30秒～99日まで指定可能です。デフォルトは[300秒]です。

● **最大クライアント接続維持時間**

クライアントからの接続を維持する最大時間を指定します。30秒～99日まで指定できます。デフォルトは[1日]です。

● **クライアントIPの通知**

要求してきたクライアントのIPアドレスをヘッダ情報としてWebサーバに通知するかどうかを指定します。デフォルトは[しない]です。

● **リクエストボディサイズの上限値**

クライアントからのリクエストボディサイズの上限値を指定します。0KB～999MBまで指定できます。0が指定されると制限無しとなります。デフォルトは[1MB]です。

● **レスポンスボディサイズの上限値**

Webサーバからのレスポンスボディサイズの上限値を指定します。0KB～999GBまで指定できます。0が指定されると制限無しとなります。デフォルトは[0(無制限)]です。

● **DNSリトライ間隔**

DNSサーバへのリトライ間隔を指定します。1秒～99秒まで指定できます。デフォルトは[3秒]です。

● **DNSリトライ数**

DNSサーバへのリトライ回数を指定します。1回～99回まで指定できます。デフォルトは[4回]です。

● **FTPのPASVモード**

FTPのPASVモードを有効にするか無効にするかを指定します。デフォルトは[有効]です。

● **FTPのパスワード**

anonymous FTP サーバへ接続する場合に、パスワード情報として送信される文字列を指定します。通常はメールアドレスを指定することが多いですが、この情報はFTPサーバに送信されるものであるため慎重に設定してください。 デフォルトは[guest@]です。

● **Viaヘッダ**

HTTPのViaヘッダを指定します。255文字まで設定可能です。指定されたヘッダの先頭には必ず「1.1 」が付きます。デフォルトは「1.1 ホスト名」です。Viaヘッダは英数字と「ー」を指定することができます。

● **キャッシュログ出力**

キャッシュログの補助出力を設定します。

● **キャッシュ有効時間**

キャッシュしたコンテンツを保持する時間を設定します。デフォルトは72時間です。

重要

- **[デフォルト値に戻す]をクリックすると、すべての設定項目をデフォルト値に戻すことができます。**
- **[設定]をクリックしないと、システムに反映されません。[デフォルト値に戻す]を行った場合も、[設定]をクリックして必ず反映してください。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

DNSサーバの設定変更は[ヘルプ]をクリックし、オンラインヘルプを参照してください。

アクセス制御設定

[プロキシ]画面の[アクセス制御設定]では、アクセス許可/禁止やキャッシュ許可/禁止、プロキシの使用許可/禁止というアクセスの制御が行えます。この設定は、最初に条件を持つリストを登録し、それぞれのリストに対しての 動作条件(アクセス制御、非キャッシュ設定、プロキシ転送)を設定していくという流れになります。デフォルトは、リスト設定に「リスト名:all，設定種別:src，条件式:0.0.0.0/0.0.0.0」、「リスト名:cgi，設定種別:url_pathregex，条件式:.cgi$ ¥?」、アクセス制御設定に「allow/deny:allow ，リスト名:all」、非キャッシュ設定に「allow/deny:deny，リスト名:cgi」です。

重要

- **アクセス制御設定において、リストをまったく設定しない場合、または指定した条件のいずれにも該当しないアクセス要求は、「アクセスを許可する」として扱われます。**
- **アクセス制御設定、非キャッシュ設定、プロキシ転送設定合わせて最大100個まで設定することが可能です。**

リスト設定

● リストの追加

リストを登録するには、アクセス制御の上画面に表示されている[リスト設定]画面から、[追加]をクリックします。

- **[追加]をクリックすることで、[リスト(追加)設定]画面を開くことができます。**
- **[リスト(追加)設定]画面で入力できるリスト名は、半角英数字16文字(先頭に数字は不可)以内です。**

- **[設定]をクリックしないと、システムに反映されませんので注意してください。**
- **設定種別や条件式の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

● リストの編集

リストを編集するには、アクセス制御の上画面に表示されている[リスト設定]画面から編集したいリスト名の左横にある[編集]をクリックします。

■リスト(編集)設定
リスト名 Method1
設定種別 Method
条件式 HTTP
設定 戻る

- [編集]をクリックすることで、[リスト(編集)設定]画面を開くことができます。
- [リスト(編集)設定]画面には、選択したリストの情報が表示されます。

- **[設定]をクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

- **リストの削除**

リストを削除するには､アクセス制御の上画面に表示されている[リスト設定]画面から削除したいリスト名の左横にある[削除]をクリックします。画面に削除するかどうかの確認を求めるダイアログボックスが表示されます。削除する場合は、[OK]をクリックしてください。

動作条件の設定

アクセス制御の下画面では、登録したリストに対して動作条件の設定を行います。3つの動作について設定することができます。

- **アクセス制御設定**

登録したリストに対して、アクセスの許可/禁止を設定します。

アクセス制御設定

追加 順序	allow/deny	リスト名
編集 削除	deny	Method1
編集 削除	deny	xxxxxxxxxxxxxx

－ アクセス制御の追加

アクセス制御リストを追加をするには、アクセス制御設定の[追加]をクリックします。

- [追加]をクリックすることで、[アクセス制御(追加)設定]画面を開くことができます。
- アクセス制御したいリストを選択し、アクセスの許可(allow)か禁止(deny)かを決定します。
- リストを複数指定した場合にはANDの処理が行われます。

重要

- **[設定]をクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

— アクセス制御の編集

アクセス制御リストを編集するには、編集したいリスト名の左横にある[編集]をクリックします。

- [編集]をクリックすることで、[アクセス制御(編集)設定]画面を開くことができます。
- [アクセス制御(編集)設定]画面には、選択したリストの情報が表示されます。

重要

- **[設定]をクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

— アクセス制御の削除

アクセス制御リストを削除するには、削除したいリスト名の左横にある[削除]をクリックします。画面に削除するかどうかの確認を求めるダイアログボックスが表示されます。削除する場合は、[OK]をクリックしてください。

— 順序の設定

アクセス制御の順序を設定することができます。[順序]をクリックすると、順序設定画面が表示されます。優先度を変更したいリストを選択し、[UP]、[DOWN]をクリックすることで設定することができます。

重要

- **順序は一番上が優先度が高く、下に行くにつれて優先度が低くなります。**
- **[実行]をクリックしないと、システムに反映されません。**

● **非キャッシュ設定**

登録したリストに対して、キャッシュしてもよい/いけないを設定します。

非キャッシュ設定		
追加 順序	allow/deny	リスト名
編集 削除	allow	Method1

－ 非キャッシュ設定の追加

非キャッシュ設定リストを追加をするには、非キャッシュ設定の[追加]をクリックします。

- [追加]をクリックすることで、[非キャッシュ(追加)設定]画面を開くことができます。
- キャッシュ制御したいリストを選択し、アクセスの許可(allow)か禁止(deny)かを決定します。
- リストを複数指定した場合にはANDの処理が行われます。

重要

- **[設定]をクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

－ 非キャッシュ設定の編集

非キャッシュ設定リストを編集するには、編集したいリスト名の左横にある[編集]をクリックします。

- **[編集]をクリックすることで、[非キャッシュ(編集)設定]画面を開くことができます。**
- **[非キャッシュ設定(編集)設定]画面には、選択したリストの情報が表示されます。**

重要

- **[設定]をクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

－　非キャッシュ設定の削除

非キャッシュ設定リストを削除するには、削除したいリスト名の左横にある[削除]をクリックします。画面に削除するかどうかの確認を求めるダイアログボックスが表示されます。 削除する場合は、[OK]をクリックしてください。

－　順序の設定

非キャッシュ設定の順序を設定することができます。[順序]をクリックすると、順序設定画面が表示されます。優先度を変更したいリストを選択し、[UP]、[DOWN]をクリックすることで設定することができます。

- **順序は一番上が優先度が高く、下に行くにつれて優先度が低くなります。**
- **[実行]をクリックしないと、システムに反映されません。**

- **プロキシ転送設定**

登録したリストに対して、隣接プロキシを使用する/しないを設定します。

プロキシ転送設定				
追加	順序	転送種別	allow/deny	リスト名
編集	削除	Always_direct	allow	xxxxxxxxxxxxxx

－　プロキシ転送設定の追加

プロキシ転送設定リストを追加するには、追加したいリスト名の左横にある[追加]をクリックします。

- [追加]をクリックすることで、[プロキシ転送(追加)設定]画面を開くことができます。
- プロキシ転送を必ず行う(Always_direct)か、行わない(Never_direct)を[転送種別]から選択します。
- それぞれの設定に対して、許可する(allow)、許可しない(deny)を設定します。
- リストを複数指定した場合にはANDの処理が行われます。

- **[設定]をクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

－ プロキシ転送設定の編集

プロキシ転送設定リストを追加をするには、プロキシ転送設定の[編集]をクリックします。

- [編集]をクリックすることで、[プロキシ転送(編集)設定]画面を開くことができます。
- [プロキシ転送設定(編集)設定]画面には、選択したリストの情報が表示されます。

重要

- **[設定]をクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

－ プロキシ転送設定の削除

プロキシ転送設定リストを削除するには、削除したいリスト名の左横にある[削除]をクリックします。画面に削除するかどうかの確認を求めるダイアログボックスが表示されます。削除する場合は、[OK]をクリックしてください。

－ 順序の設定

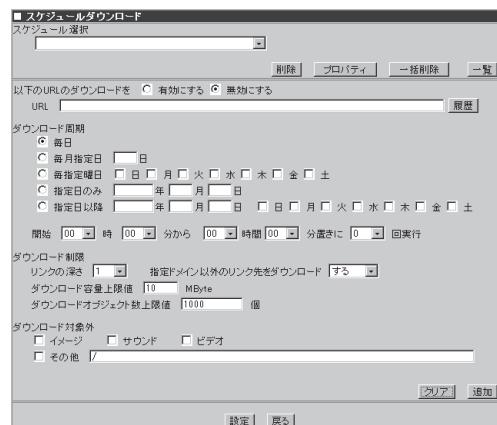
プロキシ転送設定の順序を設定することができます。[順序]をクリックすると、順序設定画面が表示されます。優先度を変更したいリストを選択し、[UP]、[DOWN]をクリックすることで設定することができます。

重要

- **順序は一番上が優先度が高く、下に行くにつれて優先度が低くなります。**
- **[実行]をクリックしないと、システムに反映されません。**

スケジュールダウンロード

スケジュールダウンロードとは、頻繁に参照されるページをあらかじめ指定時刻にダウンロードし、キャッシュに入れておく機能です。
対象となるURL、ダウンロード周期などスケジュールダウンロードの設定ができます。

重要 **コンテンツの性質とサイズによってはキャッシュされないこともあります。**

スケジュールの新規追加

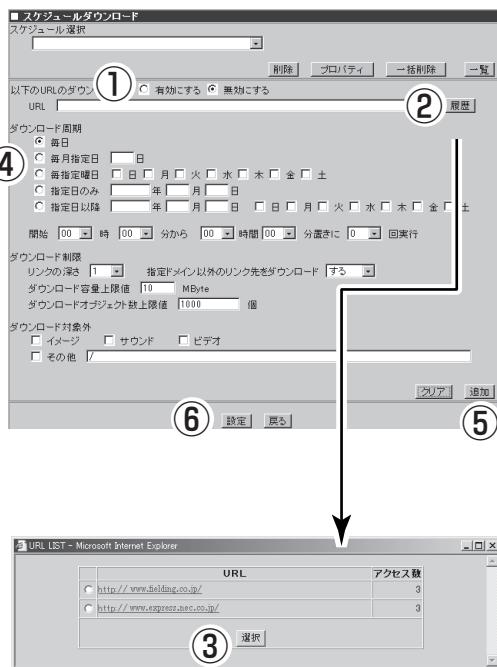
スケジュールを追加するには、対象となるURL、ダウンロード周期などを設定し[追加]をクリックします。スケジュールは最大100件まで追加できます。下に示す図と手順の流れの関係は次のとおりです。

1. 「有効にする」を選択する。
2. ダウンロードするURLを入力する。

   例） http://www.nec8.com/
3. [履歴]をクリックする。

   [URL LIST]画面が表示されます。
4. [追加]をクリックしてダウンロードしたいURLを追加する。
5. [設定]をクリックする。

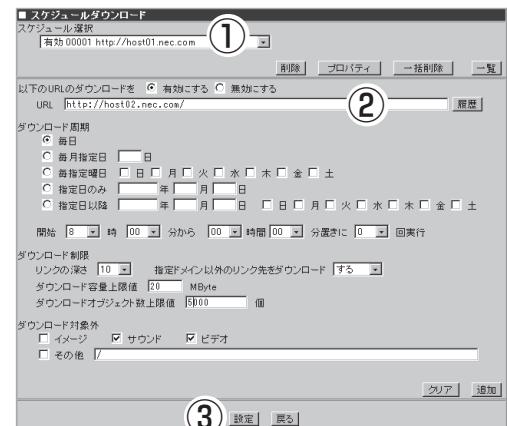
重要

- **設定項目の詳細については、[ヘルプ]をクリックしてオンラインヘルプを参照してください。**
- **履歴機能が有効になるのは、[システム]画面の[プロキシアクセス統計]でプロキシアクセス統計を「有効にする」を設定した時だけです。**

スケジュールの変更

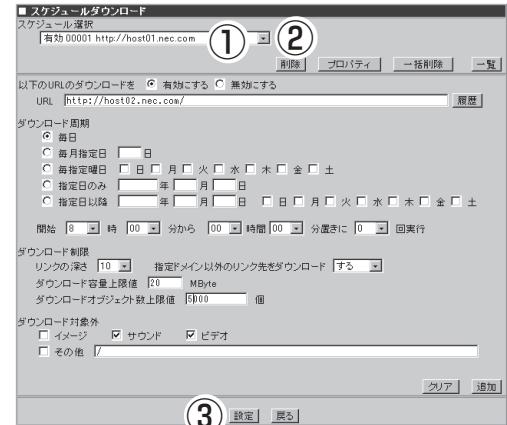
スケジュールを変更するには、[スケジュール選択]欄からスケジュールを選択し、変更したい項目を編集します。

引き続き別のスケジュールを編集するときは、そのまま一覧から選択してください。編集内容はウィンドウ内で一時保存されます。

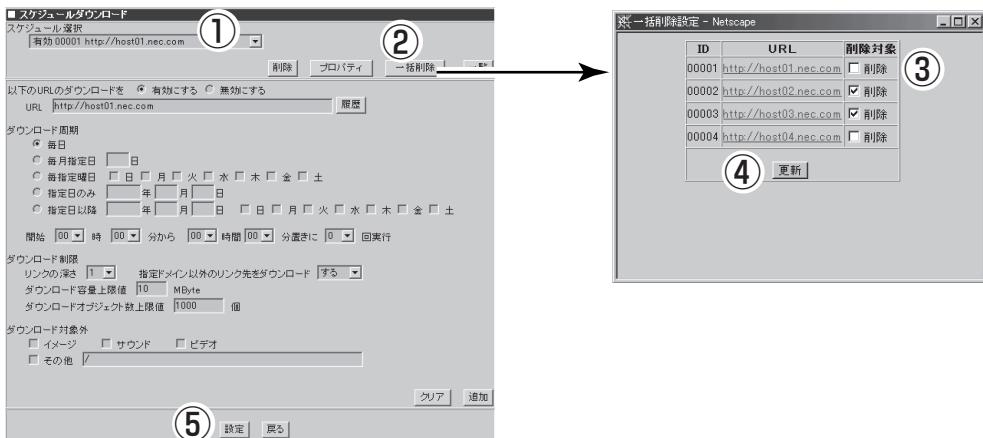
重要

- **[設定]をクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

スケジュールの削除

スケジュールを削除するには、[スケジュール選択]欄からスケジュールを選択し、[削除]をクリックします。

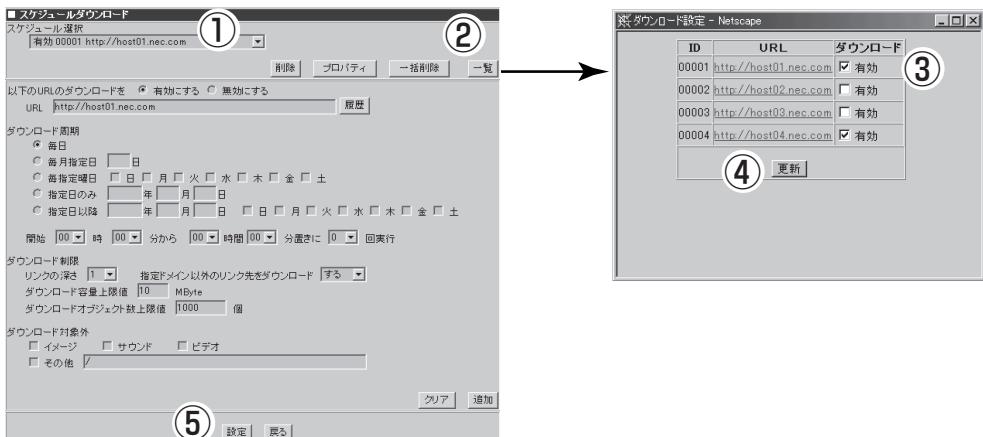
[設定]をクリックしないと、システムに反映されません。

スケジュールの一括削除

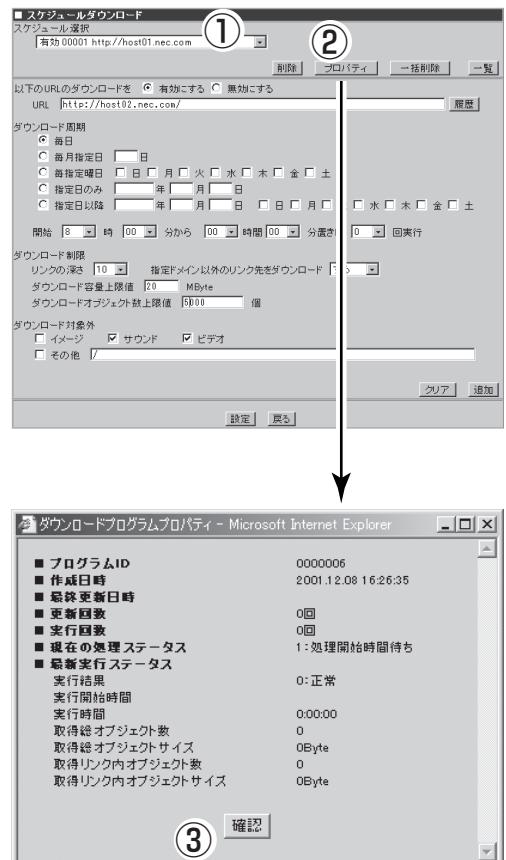
[一括削除]をクリックすることで[一括削除設定]画面を開くことができます。[一括削除設定]画面で、削除したいスケジュールの[削除対象]をチェックし[更新]をクリックすると、[スケジュール選択]欄から削除されます。

重要 **[設定]をクリックしないと、システムに反映されません。**

スケジュールの一括設定

[一覧]をクリックすることで[ダウンロード設定]画面を開くことができます。[ダウンロード設定]画面で、ダウンロードを実行したいスケジュールの[ダウンロード]をチェックし[更新]をクリックすると、[スケジュール選択]欄に反映されます。

ダウンロードを実行する時は[ダウンロード]にチェックを付け、実行しない時はチェックを外してください。

重要 **[設定]をクリックしないと、システムに反映されません。**

スケジュールの確認

[プロパティ]をクリックすると、選択したスケジュールの設定履歴や最新のダウンロード結果などを表示します。

認証設定

[プロキシ]画面の[認証設定]で、システムを使用するユーザを認証するための設定ができます。[認証設定]画面では、以下の項目を設定することができます。

- **認証方式**

  ユーザ認証を行うために使用する方式を指定します。[Ldap]と[Radius]から選択することが可能です。ユーザ認証を行わない場合は、[認証しない]を指定してください。

- **共通設定**
  - ログイン遅延時間

    LDAPサーバやRADIUSサーバへのログイン時にエラーが 発生した場合の遅延時間を指定します。
  - 認証キャッシュ有効時間

    パスワードをシステムが保持している時間を設定します。1分から99時間まで指定可能です。デフォルトは1時間です。

- **LDAP**
  - ホスト名

    LDAPサーバのホスト名(IPアドレスも可)を指定します。
  - ポート番号

    LDAPサーバとの接続に使用するポート番号を指定します。通常は389を指定します。
  - 認証フォーマット

    LDAPで認証を行う際、ユーザ名からDN(Distinguished Name)と呼ばれる識別名に変換するためのフォーマットを指定します。
  - タイムアウト時間

    LDAPサーバとの通信タイムアウト時間を指定します。デフォルトは[60秒]です。

- **RADIUS**
  - ホスト名

    Radiusサーバのホスト名(IPアドレスも可)を指定します。
  - ポート番号

    RADIUSサーバとの接続に使用するポート番号を指定します。通常は1645を指定します。
  - リトライ間隔

    RADIUSサーバへのリトライ間隔を指定します。デフォルトは[3秒]です。
  - リトライ回数

    RADIUSサーバへのリトライ回数を指定します。デフォルトは[4回]です。
  - 共有秘密鍵

    RADIUSサーバと共有する秘密鍵を指定します。RADIUSはこの秘密鍵を使って、認証応答用の識別子を生成します。
  - キャッシュサーバIPアドレス

    RADIUSサーバと通信を行うため[プロキシ]の[基本設定]画面のキャッシュサーバIPアドレスで登録されているIPアドレスを指定します。複数のIPアドレスが存在している場合は、その中の1つを指定します。

- [設定]をクリックしないと、システムに反映されませんので注意してください。
- 設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。

バイパス設定

[プロキシ]画面の[バイパス設定]では、システムを透過型プロキシとして動作させる際の、静的バイパス・動的バイパスの設定を行います。

- **静的バイパス**

  システムを透過型プロキシとして動作させる際に、指定したIPアドレスのWebサーバへのアクセス要求がシステムに来た時、システムを経由させずに直接アクセス(バイパス)させます。

  - IPアドレス

    システムを経由させず直接アクセスさせるWebサーバのIPアドレスを指定します。

- **動的バイパス**

  システムを透過型として利用する際に利用できます。指定した条件のHTTP応答をシステムが受け取った場合、今後 その応答を返したWebサーバへのアクセス要求はシステムを経由させずに直接アクセス(バイパス)させます。

  - HTTP応答コード検出

    HTTPの応答コードの種類でバイパスを行います。条件に加える応答コードをチェックしてください。また、表示されていないコードを加える場合は、その他欄に、コードの数値をカンマ区切りで入力してください。

  - HTTP以外のトラフィック検出

    HTTP以外のトラフィックをバイパスする場合はチェックを付けてください。

  - バイパス時間

    動的にバイパスを行う時間を指定します。秒単位で指定してください。

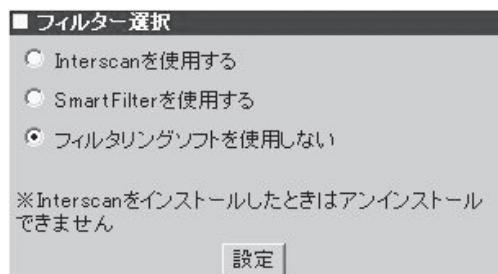
  - 動的バイパスIPの表示

    動的にバイパスされているIPアドレスまたはホスト名を表示します。

重要

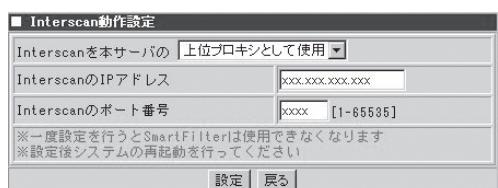
- 静的バイパスのIPアドレスを登録、変更する場合には必ず、[追加]、[編集]をクリックしてください。
- [設定]をクリックしないと、システムに反映されません。
- 上記のバイパス設定は、システムを透過型で使用した時のみ機能します。

フィルター選択

[プロキシ]画面の[フィルター選択]画面で、使用するフィルタリングソフトを選択することができます。フィルタリングソフトはInterscanとSmartFilterのいずれかを使用することができます。

SmrtFilterを使用していて、フィルタリングソフトを使用しないを設定した時、SmartFilter動作設定のSmartFilterによるフィルタリングとフィルタリングデータベースの自動更新は「実行しない」が自動的に設定されます。

- **Interscanを一度インストールするとアンインストールすることはできません。**
- **SmartFilterを使用していて、Interscanを使用したくなった場合にはいったんフィルタリングソフトを使用しないを設定してからInterscanをインストールしてください。**

Interscan設定

[プロキシ]画面の[フィルター選択]画面の[Interscan設定]で、Interscanの設定を行います。この設定はInterscanを本システムで使用するとき必ず必要です。IPアドレスとポート番号の指定はInterscanWebManagerで設定する内容に従って設定してください。なお、この画面でIPアドレスとポート番号を変更してもInterscanWebManagerには反映されません。

- Interscan設定で設定を行った後、[プロキシ]画面に[Interscan設定]の項目が表示されるようになります。
- 「Interscanを上位プロキシとして使用」を設定した時、[プロキシ]画面の[アクセス制御設定]にて設定したプロキシ転送設定が削除されます。
- 「Interscanを上位プロキシとして使用」を設定した時、[プロキシ]画面の[隣接プロキシ]設定にて設定した内容が削除されます。
- 「Interscanを上位プロキシとして使用」を設定した時、[プロキシ]画面の[親プロキシ]設定にInterscanが設定され、他の親プロキシの設定は削除されます。
- 「Interscanを上位プロキシとして使用」を設定した時、[プロキシ]画面の[認証設定]の認証方式が「認証しない」に設定され、変更できなくなります。

重要

- Interscanを一度インストールするとアンインストールすることはできません。アンインストールする場合にはシステムの再インストールを行ってください。
- システムを透過型として使用する場合にはInterscanは親プロキシとしてのみ使用可能です。
- システムをReverseプロキシとして使用する場合にはInterscanは使用できません。
- Interscanは一度インストールするとアンインストールできないため、Interscanの設定を行った後SmartFilterを使用することはできません。
- キャッシュサーバを透過型として使用する場合にはInterscanは親プロキシとして使用してください。
- InterscanWebManagerでInterscanのIPアドレスやポート番号を変更した場合には必ずこの画面の設定も変更してください。
- [Interscan設定]画面にて設定を行った場合、[システム]画面にて [システムの再起動]を実行してください。

Interscanインストール手順

Interscanのインストール手順を示します。

1. [システム]画面の[保守用パスワード]でmainteユーザのパスワードを設定します。
2. [サービス]画面で「リモートログイン(telnetd)」を起動します。
3. [サービス]画面の「リモートログイン(telnetd)」をクリックして[リモートログイン(telnetd)]画面へ遷移し、本システムにリモートログインできるようにTelnetを許可するホストを設定します。
4. Telnetでmainteユーザで本システムにリモートログインし、「su -」とコマンドラインに打ち込みます。
5. パスワードを求められるので、Management Consoleにログインするためのパスワードを指定して(adminのパスワードを指定して)管理者ユーザになります。
6. Interscanのマニュアルに基づきインストールをします。Interscanインストール中にインストールディレクトリを聞かれますが、「/usr/local」を指定します。
7. Interscanインストール後、[プロキシ]画面の[フィルター選択]で「Interscanを使用する」を指定し、「設定」をクリックして現れる[Interscan設定]画面にてInterscanのIPアドレスやポート番号を指定します。IPアドレスやポート番号を指定し、[設定]をクリックします。
8. [システム]画面にて[システムの再起動]を実行します。

SmartFilterを使用する

[プロキシ]画面の[SmartFilter設定]画面では、SmartFilterの動作設定、アクセス制限設定、サイトカスタマイズ、ユーザカテゴリ設定、エラーメッセージ設定(拒否)、エラーメッセージ設定(警告)の設定項目を選択します。

■ SmartFilter設定

設定	動作設定
設定	アクセス制限設定
設定	サイトカスタマイズ
設定	ユーザカテゴリ設定
設定	エラーメッセージ設定(拒否)
設定	エラーメッセージ設定(警告)

「SmartFilter」は30種類のブロックカテゴリ(オリジナルカテゴリとも呼ぶ)と10種類のユーザ独自のカテゴリ(ユーザカテゴリとも呼ぶ)の合計40種類のカテゴリで、最大50万件以上のサイトへのアクセスを制限することができるフィルタリングサービスです。フィルタを設定することで無駄なトラフィックや業務に無意味なアクセス、有害なホームページへのアクセスをなくし、安心できる環境でインターネットを業務や授業に利用することができます。動作設定ではフィルタリングを実行するかどうか、フィルタリングデータベース(コントロールファイルとも呼ぶ)のダウンロードのための設定などSmartFilterの動作条件を設定します。アクセス制限設定はどのような条件でアクセスの制限を行うかを設定します。サイトカスタマイズ、ユーザカテゴリ設定、エラーメッセージ設定(拒否)、エラーメッセージ設定(警告)では、よりユーザ独自のオリジナルなアクセス制限を行いたい場合にそれぞれ必要なデータの設定を行います。

SmartFilter動作設定

SmartFilterの動作設定、SmartFilterを動かすために必要なactivation key、フィルタリングデータベースのダウンロード設定、メール通知の設定、アクセスログの採取形式の選択を行います。

SmartFilterによるフィルタリングは、SmartFilterを利用したアクセス先URLのフィルタリングを実行するかどうかの設定です。activation keyは代理店より入手したactivation keyを設定します。フィルタリングデータベースの自動更新は、週に1回更新されるSmartFilterのフィルタリングデータベースを、定期的にダウンロードするかどうかの設定です。なお、フィルタリングデータベースはFTPサイトからダウンロードされるため、ユーザ名/パスワード、FTPサイト名などの設定も必要となります。メール通知設定は、コントロールリストの更新催促、およびライセンス失効時期を通知メールとして送信するための情報を設定します。カテゴリコードの付与タイプは、アクセスしたURLがカテゴリに含まれる場合に、対応するカテゴリコードをアクセスログに付与する方法を選択します。

■ SmartFilter動作設定

SmartFilterによるフィルタリング: 実行する
activation key: XXXXXXX-XXXXXXX-XXXXXXX-XXX
※SmartFilterによるフィルタリングの設定の変更を有効にするにはサーバを再起動する必要があります
設定 戻る

■ FTP設定

フィルタリングデータベースの自動更新: 実行する
以下の項目は必須です
(注意)データベースのダウンロード中はプロキシ機能が正常に動作しません
ダウンロードの実行曜日・時間: 日曜日 00 時 00 分
ユーザ名: xxxxxx
パスワード: ********
FTPサイトのホスト名: xxxx.xxxx.xxxxx..co.jp
FTPサイトのパス: /xxx/xxxxxxx
ファイル名: xxxxxxxxx
以下はFTPダウンロードをプロキシ経由で実行する場合に指定します
ホスト名: xxx.xxx.xxx.co,.jp
ポート番号: xxxxx
実行 設定 戻る

■ メール通知情報設定

メールサーバ: xxxxx.xxxxxx.xxxxxxx.xxx.co.jp
送信者メールアドレス: xxxxx@xxxx.xxxx.xxxx.co.jp
受信者メールアドレス: xxxxxx@xxxx.xxxx.xxxx.co.jp
設定 戻る

■ ログ

カテゴリコードの付与タイプ:
- 全てに付与しない
- 制限のURLにのみ付与する
- 全てに付与する

設定 戻る

設定項目「SmartFilterによるフィルタリング」で「実行する」を設定することで[プロキシ]画面[SmartFilter設定]の項目が表示されるようになります。

重要

- [設定]をクリックしないと、システムに反映されません。
- [SmartFilter動作設定]画面の[SmarFilterによるフィルタリング]の設定を変更した場合、[システム]画面にて[システムの再起動]を実行してください。
- 設定項目の詳細についてはオンラインヘルプを参照してください。

SmartFilterアクセス制限設定

アクセス制限の設定をポリシーとして登録し、各クライアントについてアクセスの許可/拒否/警告をポリシーを用いて設定を行います。ポリシー設定はポリシー名とそれに対するコメントを設定し、ポリシーに対してどのカテゴリをどの時間に制限するかを設定します。クライアント設定はクライアントのIPアドレスを指定し、指定したIPに対してどのポリシーを割り当てるかを設定します。

- ［追加］をクリックすることでそれぞれの［追加］画面を開くことができます。
- ［編集］をクリックすることで、設定されているポリシー、クライアント設定を編集することができます。
- ［削除］をクリックすることで、設定されているポリシー、クライアント設定を削除することができます。
- ［ポリシー設定］のアクセス欄の［カスタム］をクリックすることで、［ポリシーカスタム設定］画面を開くことができます。

- **クライアント設定で設定していないクライアントは接続を拒否されます。**
- **異なる複数のアクセスが同じIPに割り当てられると正しくフィルタリングされません。**

- **ポリシー設定（ポリシー追加/編集）**

ポリシー名、コメントおよびアクセスの設定を行います。ポリシー名は英数字のみ設定可能です。コメントはポリシーに対する注釈を入力することができます。アクセスは「全て許可」、「全て拒否」、「カスタム」の中から一つ選択します。アクセスを「全て許可」に設定した時、全カテゴリをすべての時間でアクセスを許可することとなります。アクセスを「全て拒否」に設定した時、全カテゴリをすべての時間でアクセスを拒否することとなります。カスタムは時間別、カテゴリ別にアクセスの許可/拒否/警告を設定することができます。

カスタムを選択し、[設定]をクリックすると、[ポリシーカスタム設定]画面が表示されます。

作成したポリシー名がすでに存在していたとき、ポリシーの追加（編集）を行うことはできません。

● ポリシーカスタム設定

カスタムは時間別、カテゴリ別にアクセスの許可/拒否/警告を設定することができます。カテゴリ選択ではカテゴリの一覧からカテゴリを選択します。選択したカテゴリのアクセス制限状況がカスタム設定の中央詳細部に表示されます。なお、カテゴリについての詳細は、オンラインヘルプの[SmartFilterの概要]画面にて参照してください。カスタム設定ではカテゴリ欄にて選択したカテゴリに対するアクセスの許可/拒否/警告を曜日、時間毎に指定します。

	日	月	火	水	木	金	土
0:00	拒否	拒否	拒否	拒否	拒否	拒否	警告
1:00	拒否	拒否	拒否	拒否	拒否	拒否	警告
2:00	拒否	拒否	拒否	拒否	拒否	拒否	警告
3:00	拒否	拒否	拒否	拒否	拒否	拒否	警告
4:00	拒否	拒否	拒否	拒否	拒否	拒否	警告
5:00	拒否	拒否	拒否	拒否	拒否	拒否	警告
6:00	拒否	拒否	拒否	拒否	拒否	拒否	警告
7:00	拒否	警告	警告	警告	警告	警告	警告
8:00	拒否	許可	許可	許可	許可	許可	警告
9:00	拒否	許可	許可	許可	許可	許可	警告
10:00	拒否	許可	許可	許可	許可	許可	警告
11:00	拒否	許可	許可	許可	許可	許可	警告
12:00	拒否	警告	警告	警告	警告	警告	警告
13:00	拒否	許可	許可	許可	許可	許可	警告
14:00	拒否	許可	許可	許可	許可	許可	警告
15:00	拒否	許可	許可	許可	許可	許可	警告
16:00	拒否	許可	許可	許可	許可	許可	警告
17:00	拒否	許可	許可	許可	許可	許可	警告
18:00	拒否	許可	許可	許可	許可	許可	警告
19:00	拒否	許可	許可	許可	許可	許可	警告
20:00	拒否	許可	許可	許可	許可	許可	警告
21:00	拒否	許可	許可	許可	許可	許可	警告
22:00	拒否	許可	許可	許可	許可	許可	警告
23:00	拒否	許可	許可	許可	許可	許可	警告

- カスタム設定の [全て許可] をクリックすることで、カテゴリ選択で選択したカテゴリに対し、全ての時間アクセスを許可する設定を行うことができます。
- カスタム設定の[全て拒否]をクリックすることで、カテゴリ選択で選択したカテゴリに対し、全ての時間アクセスを拒否する設定を行うことができます。
- カスタム設定の[全て警告]をクリックすることで、カテゴリ選択で選択したカテゴリに対し、全ての時間アクセスを警告する設定を行うことができます。
- カスタム設定下部で曜日、時間別に詳細な設定を行うことができます。

[全て許可]、[全て拒否]、[全て警告]、[設定]をクリックすることで設定が直ちに反映されます。

● クライアント設定(クライアント追加/編集)

クライアント別にポリシーの設定を行います。アクセス制限の対象となるクライアントのIPアドレスを設定し、指定したIPアドレスに対して適用したいポリシーの設定を行います。

サイトカスタマイズ

フィルタリングデータベース中のカテゴリ毎にあらかじめ定められた既定サイトのカテゴリを変更したり、アクセス制御するサイトを独自に任意のカテゴリに追加したりします。

- [追加]をクリックすることで、それぞれの[追加]画面を開くことができます。
- [編集]をクリックすることで、設定されているURL、カテゴリを編集することができます。
- [削除]をクリックすることで、チェックボックスが選択されているURL、カテゴリを全て削除することができます。

重要

アクセスを制御するために登録したサイトが既に何らかのカテゴリに属している場合でも、そのサイトについてユーザが定義したカテゴリが優先されます。

- **サイト追加/編集**

URL、アクセス可否および登録するカテゴリの設定を行います。URLは、アクセス制御の対象とするURLをhttp://を除いた形式で指定します。アクセス可否は、指定したサイトのアクセスを許可するまたは許可しないを選択します。カテゴリは、[許可しない]を選択した場合のみ有効であり、指定したサイトのアクセスを制御するカテゴリを選択します、設定方法の詳細は、オンラインヘルプを参照してください。

- [サイト追加]画面では、[URL]に複数のURLが指定できます。複数指定する場合には、各URLの間をセミコロン(;)で区切ります。
- [サイト編集]画面では、[URL]に複数のURLは指定できません。ただし、変更は可能です。
- [アクセス拒否]で[許可しない]を選択した場合、登録するカテゴリは複数選択可能です。

ユーザカテゴリ設定

フィルタリングデータベース中の30個のオリジナルカテゴリ以外に提供されている10個のユーザ独自のカテゴリ(ユーザカテゴリ)に対する設定を行います。ユーザカテゴリ設定は、ユーザカテゴリのカテゴリ名を変更します。

エラーメッセージ設定(拒否)

アクセスを拒否すると設定されているサイトにアクセスした際に表示される拒否メッセージをカテゴリ毎に変更することができます。

サイトが複数のカテゴリに属する場合は、そのサイトが属するカテゴリのいずれかのメッセージが表示されます。

右に「拒否」指定カテゴリのサイトにアクセスした際のデフォルトメッセージ画面を示します。

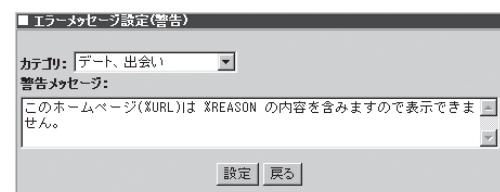
[拒否メッセージ]で編集した場合の例を示します。

エラーメッセージ設定(警告)

アクセスを警告すると設定されているサイトにアクセスした際に表示される警告メッセージをカテゴリ毎に変更することができます。

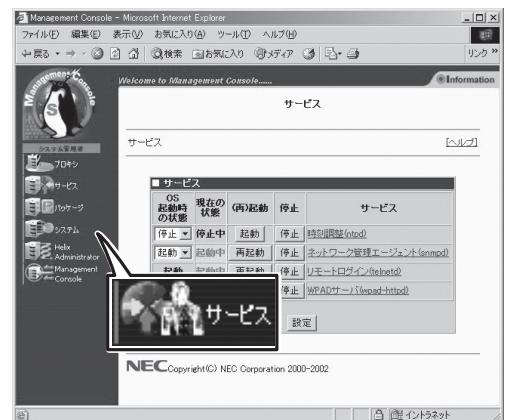
サイトが複数のカテゴリに属する場合は、そのサイトが属するカテゴリのいずれかのメッセージが表示されます。

右に「警告」指定カテゴリのサイトにアクセスした際のデフォルトメッセージ画面を示します。

[警告メッセージ]で編集した場合の例を示します。

サービス

管理者は、Management Consoleから以下のサービスの設定を簡単に行うことができます。

- 時刻調整（ntpd）
- ネットワーク管理エージェント（snmpd）
- リモートログイン（telnetd）
- WPADサーバ（wpad-httpd）

  サービス画面では各機能の停止・起動を指示可能で、現在の稼動状況を表示します。さらにここから、各機能ごとの詳細な設定を行う画面に移ります。

－ OS起動時の状態:　システムが起動した際に、このサービスを自動的に有効にするかどうかを指定します。

－ 現在の状態:　現在、このサービスが動作しているかどうかを表示します。

－ （再）起動:　このサービスが停止している場合に起動します。動作中の場合には、停止させてから再起動します。

－ 停止:　このサービスが動作中であれば、停止します。

【サービスの画面構成】

■ サービス画面

- 時刻調整（ntpd）
  - 同期ホスト一覧
    - □　時刻同期ホスト追加
    - □　時刻同期状況の確認
    - □　日時・時刻
- ネットワーク管理エージェント（snmpd）
  - コミュニティ一覧
    - □　コミュニティ追加
    - □　コミュニティ編集
  - システム情報
  - 認証トラップ
  - トラップ送信先一覧
    - □　トラップ送信先
- リモートログイン（telnetd）
  - Telnetログインを許可するホスト
- WPADサーバ（wpad-httpd）
  - プロキシサーバ自動設定ファイル

時刻調整(ntpd)

NTP(Network Time Protocol)は、ネットワークで接続されたコンピュータ同士が連絡を取り合い、時計のずれを自動的に調整する仕組みです。本システムはこの仕組みを利用して、以下の機能を提供しています。

- インターネットの標準時刻サーバに、本システムの時計を合わせせる。
- 他のPCが時計を本システムに合わせせるのに必要な情報を提供する。

【画面ごとの説明】

- **同期ホスト一覧**

本システムがNTPを使って連絡を取り合う標準時刻サーバあるいは PC(以降ホストと略記)の一覧を表示します。

ー　追加

「時刻同期ホスト追加」画面に遷移します。

ー　削除

ボタンに対応するホストを一覧から削除します。

ー　時刻同期状況の確認

「時刻同期状況の確認」画面に遷移します。

- **時刻同期ホスト追加**

本システムがNTPを使って連絡を取り合うホストの追加登録を行います。

ー　別ホストと同期

ネットワークに接続されている他のホストと同期する場合に選択します。これが選択されている場合、以下が有効になります。

タイプ
server/peerのいずれかを指定します。

IPアドレス/ホスト名
ホストをIPアドレスあるいはホスト名で指定します。

ー　ローカルで同期

別のホストを指定せず、自身で同期を行う場合に選択します。

- **時刻同期状況の確認**

登録されているホストとの間での時刻同期の状況を表示します。

■ 時刻同期状況の確認

remote	refid	st	t	when	poll	reach	delay	offset	jitter
xx.xxx.xxx	0.0.0.0	16	u	-	64		0.000	0.000	4000.00

● 日付・時刻

このページを開いた時点の日時を表示します。[設定]をクリックすると、今表示されている時刻をシステムに設定します。

ネットワーク管理エージェト(snmpd)

SNMP(Simple Network Management Protocol)は、ネットワークに接続された機器の稼動状況を、ネットワークを通じて取得するための仕組みです。本システムは、ネットワークに接続された機器(エージェント)の側として、必要な情報をネットワークに発信する機能を提供しています。

【画面ごとの説明】

● コミュニティ一覧

このネットワークエージェントにアクセス可能な管理マネージャマシンの一覧を表示します。またここから登録・変更・削除をします。

■ コミュニティ一覧

操作	コミュニティ名	許可するアドレス	管理対象MIB
追加			
編集 削除	public	default	システム

ー　追加

コミュニティを新規追加する画面に遷移します。

ー　編集

ボタンの右隣にあるコミュニティの設定を変更する画面に遷移します。

ー　削除

ボタンに対応するコミュニティを一覧から削除します。

● システム情報

このマシンが設置されている場所や管理者のメールアドレスなどを記入しておいてください。この情報は必要に応じて管理マネージャから読み取られます(日本語を用いると、マネージャ側で文字が化けることがあります)。

● 認証トラップ

不正な管理マネージャが不正なコミュニティ名でアクセスしてきたときに、その旨を正規の管理マネージャに通知するかどうかを指定します。

■ 認証トラップ

☑ 認証トラップを生成する

設定

● **トラップ送信先一覧**

このマシンに何らかの障害が発生した際に、トラップメッセージを送信する先(管理マネージャ)の一覧を登録します。

－　追加

トラップ送信先を新規追加する画面に遷移します。

－　編集

ボタンの右隣にあるトラップ送信先の設定を変更する画面に遷移します。

－　削除

ボタンに対応するトラップ送信先を一覧から削除します。

リモートログイン(telnetd)

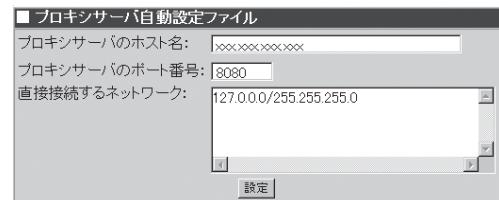
Management Consoleより原初的な手段で、他のコンピュータ(ホスト)から本システムに接続することを可能にする機能です。Management Consoleでは対応できない特別な操作を行いたい場合にだけこの機能を有効にします。通常の運用時に有効にする必要はありません。有効にしている間はセキュリティのレベルが低下しますので、通常は無効にしておくことをお勧めします。

「Telnetログインを許可するホスト」画面にて、ログイン可能なホストを各種形式で指定します。カンマで区切って複数のホストを指定可能です。IPアドレスやホスト名以外にも各種指定形式をサポートしています。指定形式の詳細についてはヘルプを参照してください。

重要

- **[システム]画面の[保守用パスワード]にてパスワードを設定後、「mainte」ユーザでリモートログインが可能となります。**
- **初期導入設定直後の「Telnetログインを許可するホスト」は、初期導入設定用ディスクに指定したIPアドレスとサブネットマスクをもとに、当該ネットワークからの接続のみを許可するように設定されます。**

WPADサーバ(wpad-httpd)

本システムをフォワードプロキシとして利用している際に、ブラウザ側でのプロキシ設定を自動化するための機能です。Internet Explorer 5以降で対応しています。本機能を利用するためには、ブラウザの参照しているDNSサーバおよびDHCPサーバを適切に設定する必要があります。

[プロキシサーバ自動設定ファイル]画面で本システムに接続する際に使用するホスト名とポート番号を設定します。本システムを通さないで接続すべきマシンがあれば、ネットワークアドレス単位で指定することが可能です。

- **プロキシサーバのホスト名**

  ホスト名またはIPアドレスを指定します。

- **プロキシサーバのポート番号**

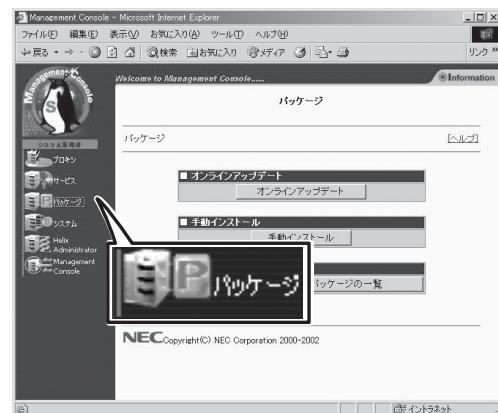
  ポート番号を指定します。

- **直接接続するネットワーク**

  ブラウザが本システムを経由しないで直接接続すべきネットワークを指定してください。

重要 WPADサーバは本システムのサーバ種別を「Forward(透過型L4スイッチ)」、「Forward(透過型WCCP)」または「Reverse」に設定した時にはご利用できません。

パッケージ

本システムにインストールされているアプリケーションなどのソフトウェアパッケージのアップデートやインストール、インストールされているパッケージの一覧を確認する画面です。

オンラインアップデート

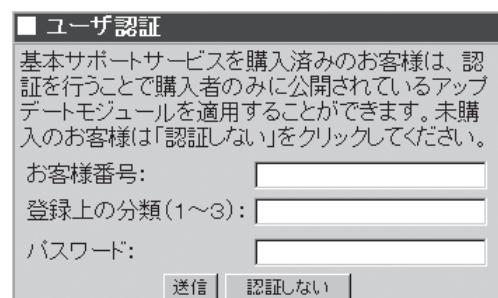
オンラインアップデートを利用すると、ManagementConsoleから安全にアップデートモジュールをインストールすることができます。

■ オンラインアップデート
オンラインアップデート

アップデートモジュールとは、本システムに追加インストール(アップデート)可能なソフトウェアで、弊社で基本的な動作確認を行って公開しているものです。 内容は、既存ソフトウェアの出荷後に発見された不具合修正や機能追加などが主ですが、新規ソフトウェアが存在することもあります。オンラインアップデートでは、現在公開されている本システム向けのアップデートモジュールの一覧を参照し、安全にモジュールをインストールすることができます。

● **ユーザ認証**

初めてオンラインアップデートを利用する場合、また公開モジュールの最新情報を取得する場合、[ユーザ認証]画面が表示されます。ここで、基本サポートサービスをご購入されたお客様は、基本サポ ートサービスのお客様番号・分類・パスワードを入力してください。未購入のお客様は[認証しない]をクリックして進んでください。

■ ユーザ認証
基本サポートサービスを購入済みのお客様は、認証を行うことで購入者のみに公開されているアップデートモジュールを適用することができます。未購入のお客様は「認証しない」をクリックしてください。
お客様番号:
登録上の分類(1～3):
パスワード:
送信 認証しない

● **アップデートモジュール一覧**

公開されているアップデートモジュールの一覧が表示されます。本装置向けのモジュールで、まだインストールされていないモジュールのみが表示されます。各モジュールの機能や修正情報などを確認することができます。

■ アップデートモジュール一覧

日付	概要	パッケージ名	適用	操作
2000/xx/xx	telnet パッケージのアップデート [詳細情報]	telnet-0.17-xx	未	適用
2001/xx/xx	WPADサーバ修正モジュール [詳細情報]	wpad-httpd-1.00-xx	未	適用
2001/xx/xx	Management Console 機能強化モジュール [詳細情報]	wbmccache-1.0-xx	未	適用
2001/xx/xx	CacheServer カーネルアップデートモジュール [詳細情報]	kernel-2.4.3-xx	未	適用
		roma-1.0-xx	未	
		catfish-1.01-xx	未	

モジュールは、実際は主にRPMパッケージ形式で提供されるファイルですが、1つの機能のために複数のRPMパッケージを必要とする場合もあり、その場合は複数ファイルで構成されています。[適用]をクリックすると、該当モジュールのインストール作業を開始します。

● **信頼性の確認**

「適用」をクリックすると、該当モジュールのインストールに必要なファイルをすべて取得します。ファイルのサイズが大きい場合は、時間がかかる場合があります。ファイルの取得が完了し、一時ディレクトリに保管した後、ファイルが正しく転送されたかどうかを自動的に検査します。検査にはMD5メッセージ・ダイジェストを用います。

検査に合格した場合は、画面に各ファイルのMD5メッセージ・ダイジェストが表示されます。最終的な確認として、弊社アップデートモジュール公開Webサイトで参照できる各ファイルのMD5メッセージ・ダイジェストの文字列と比較し、同じかどうか確認してください。[OK]をクリックするとインストールを実行します。

手動インストール

ローカルディレクトリのファイル名、またはURL、PROXY、PORTを指定してRPMパッケージをインストールすることができます。詳細は画面上の[ヘルプ]をクリックしオンラインヘルプを参照してください。

■ 手動インストール

手動インストール

● **ローカルディレクトリ指定**

本システムへCD-ROMからRPMパッケージをインストールする場合、CD-ROMドライブにRPMの入ったCD-ROMをセットし、この画面よりインストールしたいRPMパッケージを選んで追加してください。

● URL指定

本システムがすでにインターネットに接続されている場合には、RPMパッケージの置かれているサイトのURLを指定してそこからダウンロードしインストールを行うことができます。

● PROXY指定

プロキシ経由でRPMパッケージをダウンロードする場合に、プロキシサーバのアドレスを指定することができます。

● PORT指定

プロキシ経由でRPMパッケージをダウンロードする場合に、プロキシサーバのポート番号を指定することができます。

インストールする場合には、必ず[追加]をクリックしてください。

パッケージの一覧

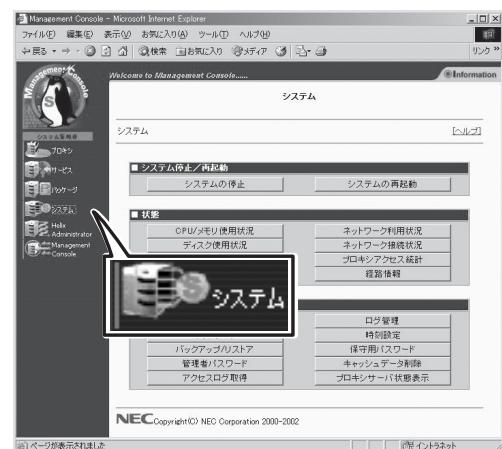
現在本システムにインストールされているRPMパッケージの一覧を確認することができます。また、アンインストール作業を行うこともできます。詳細は画面上の[ヘルプ]をクリックしオンラインヘルプを参照してください。

■ パッケージの一覧
インストールされているパッケージの一覧

■ パッケージ一覧

グループ	パッケージ名	概要
Applications/Publishing	ghostscript-fonts-5.50-3	Fonts for the Ghostscript PostScript(TM) interpreter.
Documentation	indexhtml-7.1-2	The Web page you'll see after installing Red Hat Linux
Applications/System	kon2-fonts-0.3.9b-6	Fonts for KON
System Environment/Base	mailcap-2.1.4-2	Associates helper applications with particular file types.
Documentation	man-pages-ja-0.4-3	Japanese man (manual) pages from the Linux Documentation Project
Development/Libraries	pump-devel-0.8.11-1	Development tools for sending dhcp requests
System Environment/Base	redhat-release-7.1-1	Red Hat Linux release file
System Environment/Base	filesystem-2.0.7-1	The basic directory layout for a Linux system.
System Environment/ Libraries	glibc-2.2.2-10	The GNU libc libraries.
Development/Tools	byacc-1.9-18	A public domain Yacc parser generator.
Development/Tools	cproto-4.6-7	Generates function prototypes and variable declarations from C code.
Development/Tools	ctags-4.0.3-1	A C programming language indexing and/or cross-reference tool.
Development/Libraries	db1-devel-1.85-5	Development libs/header files for Berkeley DB (version 1) library.
Development/Libraries	db2-devel-2.4.14-5	Development libs/header files for Berkeley DB (version 2) library.
System Environment/ Libraries	db3-devel-3.1.17-7	Development libraries/header files for the Berkeley DB library.
Applications/Communications	dip-3.3.7o-22	Handles the connections needed for dialup IP links.

システム

Management Console画面左の[システム]アイコンをクリックすると「システム」画面が表示されます。

システム停止／再起動

[システム]画面の[システム停止／再起動]一覧から[システムの停止]、および[システムの再起動]を実行できます。

システムの停止

[システムの停止]をクリックすると「システムを停止します。よろしいですか?」とダイアログボックスが表示されます。停止する場合は[はい]を、停止したくない場合は[キャンセル]をクリックしてください。
[はい]をクリックすると、終了処理をした後、システムの電源がOFFになります。本体前面のPOWERランプが消灯したことを確認してください。

システムの再起動

[システムの再起動]をクリックすると「システムを再起動します。よろしいですか?」とメッセージが表示されます。再起動する場合は[はい]を、停止したくない場合は[キャンセル]をクリックしてください。
[はい]をクリックすると、終了処理をした後、システムがいったん停止し、再起動します。

状　態

［システム］画面の［状態］一覧から以下のシステム状態を確認できます。

● CPU／メモリ使用状況

メモリの使用状況とCPUの使用状況をグラフと数値で表示します。約10秒ごとに最新の情報に表示が更新されます。

● ディスク使用状況

ディスクの使用状況を各ファイルシステムごとに数値とグラフで表示します。空き容量、使用率に注意してください。空き容量が足りなくなるとシステムが正常に動作しなくなる可能性があります。

● プロセス実行状況

現在実行中のプロセスの一覧を表示します。プロセス実行状況の表の最上行の項目名をクリックすると、各項目で表示をソートすることができます。表示項目の詳細については、［ヘルプ］をクリックし、オンラインヘルプを参照してください。

● 名前解決診断

ネットワーク設定で登録されているDNSサーバの動作を確認することができます。
「ホスト:」に適当なホスト名を入力して［診断］をクリックすると診断結果が表示されます。ホスト名に対して正しく「Name:」と「Address:」が表示されればDNSサーバは正常に機能しています。

● ネットワーク利用状況

ネットワーク利用状況を表示します。
［約5秒毎に画面をリフレッシュする］チェックボックスをチェックすると自動的に表示が最新状況に更新されます。

● ネットワーク接続状況

各ポートごとの接続状況を表示します。

［約5秒毎に画面をリフレッシュする］チェックボックスをチェックすると自動的に表示が最新状況に更新されます。

- **プロキシアクセス統計**

アクセスの統計情報を表示します。「Summary by Month」の表の[Month]の項目のリンクをクリックするとその月の詳細な統計情報を表示します。

プロキシアクセス動作設定はプロキシアクセス統計を有効にして動作させるかどうか設定します。

動作させる際には優先度を設定してください。優先度は1から20まで設定可能であり、値が大きいほど優先度が低くなります。優先度を低くすることによりプロキシアクセス統計の動作によるCPUの負荷を減らすことができます。

Webalizer表示設定では、sitesはサイト別上位を、sites By KBytesはサイト別キロバイト上位を、URL'sはURL上位を、URL' s By KBytesはサイト別キロバイト上位をEntry Pagesは入り口上位を、Exit Pagesは出口別上位をいくつまで表示するか設定することができます。

■ プロキシアクセス動作設定

プロキシアクセス統計	○ 有効にする ◉ 無効にする
優先度	1

※無効にするを選択すると統計情報は削除されます
※優先度は慎重に決定して下さい
[設定]

■ プロキシアクセス統計表示

統計情報は作成されていません

■ プロキシアクセス統計設定

統計情報が以下のサイズを越えたら、情報をクリアします
10 MB （現時点では 統計情報は作成されていません）
[設定]

■ Webalizer表示設定

Sites:	31
Sites By KBytes:	10
URL's:	30
URL's By KBytes:	10
Entry Pages:	10
Exit Pages:	10

[初期値] [設定] [戻る]

- [初期値]をクリックすると、それぞれのテキストボックスに初期値が入ります。
- 各テキストボックスは2桁まで入力することができます。
- 統計情報はシステムのアクセスログがローテートされたときに作成されます。
- システムのアクセスログのローテートの設定は[システム]画面の[ログ設定]画面の[キャッシュサーバアクセスログ]の[設定]をクリックすることで表示される[キャッシュサーバアクセスログ設定]画面にて行えます。

重要

- **プロキシアクセス統計を無効にするを選択するとそれまで作成されていた統計情報は削除されます。**
- **プロキシアクセス統計を動作させると性能低下がおこる可能性があります。**
- **優先度は慎重に決定してください。低い優先度を設定するとシステムの負荷状況によっては正常に統計情報が作成されない可能性があります。**
- **プロキシアクセス統計情報を動作させると、キャッシュサーバのアクセスログのログ出力形式はSquidに、ローテート世代数は「1」に固定され、ローテートサイズはいったん100MBに設定されます。**
- **プロキシアクセス統計を動作させている時、ローテートサイズの扱いには注意してください。システムの性能およびプロキシアクセス統計の動作に影響を与えます。**

- **経路情報**

「相手ホスト:」にホスト名を入力して[表示]をクリックすると、そのホストまでの経路情報を表示します。

その他

［システム］画面の［その他］一覧から、以下の機能を利用できます。

● **システム情報**

装置に割り当てたホスト名、およびOSに関する情報を表示します。

● **ネットワーク**

ネットワークの基本的な設定やネットワークインタフェース、ルーティングの設定を行います。

－　基本設定
ホスト名、ドメイン名、デフォルトゲートウェイ、パケットフォワーディング、ＤＮＳの設定を行います。DNSは複数設定可能であり、順序を入れ替えることができます。

－　ネットワーク設定

［ネットワーク設定］画面では、下記2項目が選択でき、選択するとおのおのの設定画面を表示します。

□ インタフェース

本システムは複数のネットワークインタフェースを利用できます。これらインタフェースそれぞれに、複数のIPアドレスを割り当てて、複数のネットワークに所属させることが可能になっています。インタフェース毎に現在割り当てられている情報の一覧を表示します。また、ここから追加・編集・削除操作を行います。

□ ルーティング
ルーティングテーブルの追加・編集・削除操作を行います。

■ ルーティング

処理	宛先	サブネットマスク	ゲートウェイ	フラグ	インタフェース名
追加					
編集 削除	zzz.zzz.1.1	255.255.255.0	zzz.zzz.1.254	UGH	eth0
	xxx.xxx.0.1	255.255.255.0	0.0.0.0	U	eth0
	xxx.xxx.1.1	255.255.255.0	0.0.0.0	U	eth0
	yyy.yyy.0.1	255.255.255.0	0.0.0.0	U	eth1
	127.0.0.0	255.0.0.0	0.0.0.0	U	lo
	0.0.0.0	0.0.0.0	100.8.45.254	UG	eth0

● バックアップ/リストア

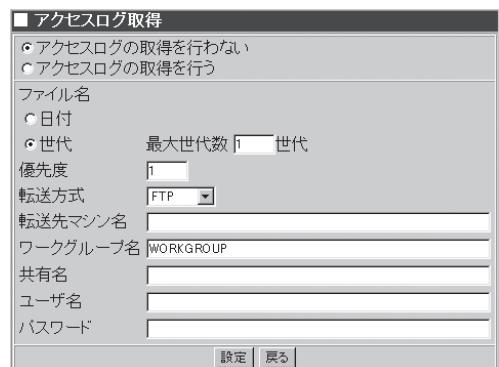
ファイルのバックアップおよびリストアの設定を行います。詳細はこの後に説明する「バックアップ/リストア」を参照してください。

● 管理者パスワード

管理者(admin)のパスワードを変更します。また、管理者宛のメールを転送する先を設定できます。管理者宛メールの転送先は正しく送信できるアドレスを指定してください。各パスワードは6文字以上8文字以下の半角英数文字(半角記号を含む)を指定してください。省略すると、パスワードは変更されません(空のパスワードを指定することはできません)。

● アクセスログ取得

キャッシュサーバアクセスログをSambaまたはFTPで指定したホストを利用して転送します。

ファイル名の形式は日付、世代のいずれかを選択できます。[ファイル名]で[日付]を選ぶとaccess(日付).log、[世代]を選ぶとaccess(世代).logとなります。

アクセスログ取得を動作させる際には優先度を設定してください。優先度は1から20まで設定可能であり、値が大きいほど優先度が低くなります。優先度を低くすることによりアクセスログ取得の動作によるCPUの負荷を減らすことができます。

重要

- **アクセスログ取得を行っている時、[システム]画面の[ログ管理]画面のキャッシュサーバアクセスログのログの世代数は「1」に固定されます。**
- **アクセスログ取得、プロキシアクセス統計情報を動作させている時はローテートサイズの扱いに注意してください。システムの性能に影響を与えます。**
- **アクセスログ取得を動作させると性能低下がおこる可能性があります。**
- **優先度は慎重に決定してください。低い優先度を設定するとシステムの負荷状況によっては正常に統計情報が作成されない可能性があります。**
- **アクセスログの転送はログのローテートが行われるタイミングで実行されます。**
- **本システムのアクセスログのローテートの設定は[システム]画面の[ログ管理]画面の[キャッシュサーバアクセスログ]の[設定]をクリックすることで表示される[キャッシュサーバアクセスログ設定]画面にて行えます。**

- **ログ管理**

ログの表示、ログのローテートの設定を行います。

ログの表示は表示したいログの[表示]をクリックするとローテートされたログの一覧が表示され、その中から表示したいログを選択して表示します。

ログのローテートの設定は、ローテートを行うタイミングを周期またはファイルサイズで指定し、何世代までログを残すかを設定します。

■ ログ管理

操作	ログファイル	ローテート	世代
表示 設定	キャッシュサーバアクセスログ	400Mbyteごと	4
表示 設定	コントロールリストのダウンロードログ	1000byteごと	2
表示 設定	システムログ		
表示 設定	システムのセキュリティログ		
表示 設定	システムのメールログ		
表示 設定	システムのブートログ		
表示 設定	クーロンログ		
表示	キャッシュログ		
表示 設定	WPADサーバログ		
表示 設定	WCCPログ		
表示 設定	Management Consoleログ	毎週	5
表示 設定	Management Consoleのアクセスログ	毎月	5
表示 設定	Management Consoleのエージェントログ	毎月	5
表示 設定	Management Consoleのエラーログ	毎月	5
表示 設定	Management Consoleの参照ログ	毎月	5

ログを表示したとき、ログのダウンロードを行うことも可能です。

重要

- **ログのローテートは毎日0:00とシステム起動時にチェックし、条件があっているものをローテートします。**
- **ログのローテートのタイミングでシステムの停止および再起動を行う場合にはご注意ください。**
- **キャッシュサーバアクセスログの設定は他のログと異なります。詳細は次に説明する「キャッシュサーバアクセスログ」を参照してください。**

ー　キャッシュサーバアクセスログ

キャッシュサーバアクセスログの[設定]をクリックすると、[キャッシュサーバアクセスログ設定]画面が表示されます。この画面は、キャッシュサーバアクセスログの出力形式、ローテート(条件、サイズ、時間、時刻)、何世代までログを残すかなどを設定することができます。出力形式が拡張形式であったとき、拡張形式でチェックボックスにチェックを入れた項目がログ出力されます。

重要

- **プロキシアクセス統計情報を有効にしている時は出力形式はSquid、世代数は「1」に固定され、ローテートサイズはいったん100MBに設定されます。**
- **アクセスログ取得を行っている時、世代数は「1」に固定されます。**
- **アクセスログ取得、プロキシアクセス統計情報を動作させている時はローテートサイズの扱いに注意してください。システムの性能に影響を与えます。**
- **拡張形式の設定項目 フィルタリング結果,フィルタカテゴリはSmartFilter動作時のみ表示されます。**

アクセスログのフォーマット

アクセスログは、2つの形式から選択し、出力することができます。それぞれの出力内容は以下のようになります。

● Squid形式

出力例: 989605543.072 89 xxx.xxx.xxx.xxx TCP_HIT/200 7653 GET http://www.foobar.com/ - DIRECT/proxy.xxx.xx.jp
①②③④⑤⑥⑦⑧⑨

text/html ALLOW Art/Culture
⑩⑪⑫

各出力項目を説明します。

① タイムスタンプ ー データオブジェクトの取得処理が完了した時間です。UNIX時間(1970年1月1日からの秒数)で出力します。
② 経過時間 ー データオブジェクトの取得処理にかかった時間をミリ秒で出力します。
③ クライアントアドレス ー クライアントのIPアドレスを出力します。
④ ログタグ／HTTPコード番号 ー システムがどのように要求を処理したかを表すタグ名と、HTTPのステータスコードを出力します。
⑤ サイズ ー データオブジェクトのサイズをバイトで出力します。
⑥ 要求方法 ー HTTPの要求方法を出力します。
⑦ URL ー 要求されたURLを出力します。
⑧ 出力無し ー 必ず「ー」が出力されます。
⑨ 階層構造データタグ／ホスト名 ー オブジェクトの取得がどのように行われたかを表すタグ名と、取得したサーバ名を出力します。
⑩ コンテンツタイプ ー オブジェクトデータのコンテンツタイプを出力します。
⑪ フィルタリング結果を出力します。(SmartFilter有効時のみ)
⑫ URLの属するカテゴリを出力します。(SmartFilter有効時のみ)

● 拡張形式

出力例: 2001-12-04 16:34:36 xx.xx.xx.xx - yy.yy.yy.yy sss GET http://www.foobar.com/ - - HTTP/1.0 200 837
①②③④⑤⑥⑦⑧⑨⑩⑪⑫

147 188 "AAA/Browser(aaa)" "" "" HIT - - ALLOW Art/Culture
⑬⑭⑮⑯⑰⑱⑲⑳㉑㉒

各出力項目を説明します。

① 日付と時刻
② クライアントのIPアドレス
③ ユーザー名(認証機能を使用した時のみ出力されます)
④ キャッシュサーバIPアドレス
⑤ リバースプロキシ動作時のホスト名(またはIPアドレス)
⑥ HTTPの要求方法
⑦ URL
⑧ URLステム ー URLに「?」が含まれた場合、「?」までのURLを出力します。
⑨ URLクエリー ー URLに「?」が含まれた場合、「?」以降のURLを出力します。
⑩ HTTPバージョン
⑪ HTTPステータスコード
⑫ データオブジェクトサイズ(バイト)
⑬ リクエストサイズ(バイト)
⑭ 経過時間
⑮ ユーザーが使用したブラウザ情報
⑯ 参照URL
⑰ 発信元クライアントIPアドレス
⑱ キャッシュHIT/MISS
⑲ 連携プロキシIPアドレスープロキシ階層がある場合は、リクエストを送信した連携プロキシのIPアドレスを出力します。
⑳ WEBサーバIPアドレスープロキシ階層が無い場合は、リクエストを送信したWEBサーバのIPアドレスを出力します。
㉑ フィルタリング結果を出力します。(SmartFilter有効時のみ)
㉒ URLの属するカテゴリを出力します。(SmartFilter有効時のみ)

*1 ③～㉒の項目は、出力の有無をユーザーが選択することが可能です。
*2 詳細な説明は、オンラインヘルプを参照してください。

- **時刻設定**

  本章の「時刻調整(ntpd)」を参照してください。

- **保守用パスワード**

  保守用ユーザー(mainte)のパスワードを設定します。設定後、「mainte」ユーザでリモートログイン(Telnet)サービスを利用することができます。パスワードは6文字以上8文字以下の半角英数字(半角記号を含む)を指定してください。省略するとパスワードは変更されません。また空のパスワードを指定することはできません。

- **キャッシュデータ削除**

  本製品がハードディスク上にキャッシュしているWebコンテンツ等を削除することができます。

- **プロキシサーバ状態表示**

  [システム]画面の[プロキシサーバ状態表示]では、プロキシサーバに関するさまざまな情報を確認することができます。[プロキシサーバ状態表示]画面は、以下の7つに分類され、それぞれの項目をクリックすることで、関連する詳細な情報を確認できます。また、それぞれの画面は一定時間ごとに最新情報に更新されます。

  - 一般情報

    [一般情報]をクリックすると、[プロキシサーバ状態表示(一般情報)]画面が表示されます。この画面では、プロキシサーバのバージョン情報や、運用時間等を確認することができます。

  - キャッシュ概要

    [キャッシュ概要]をクリックすると、[プロキシサーバ状態表示(キャッシュ概要)]画面が表示されます。この画面では、システムの現在の動作状況等を確認することができます。

  - キャッシュ情報

    [キャッシュ情報]をクリックすると、[プロキシサーバ状態表示(キャッシュ情報)]画面が表示されます。この画面では、一定時間あたりのシステムへの接続数や、リクエスト数等を確認することができます。

  - クライアント要求

    [クライアント要求]をクリックすると、[プロキシサーバ状態表示(クライアント要求)]画面が表示されます。この画面では、システムが起動開始から現時点までに処理したさまざまな情報を確認することができます。

  - ICP情報

    [ICP情報]をクリックすると、[プロキシサーバ状態表示(ICP情報)]画面が表示されます。この画面では、隣接プロキシと関連する情報を確認することができます。

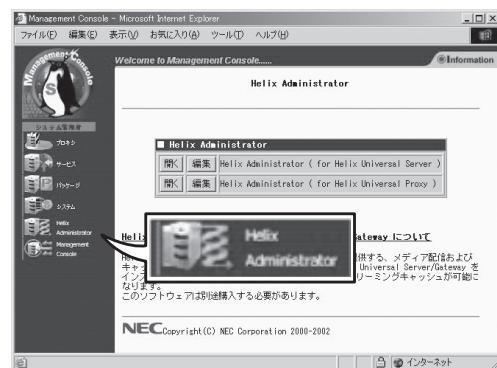
－　CERN情報

[CERN情報]をクリックすると、[プロキシサーバ状態表示(CERN情報)]画面が表示されます。この画面では、親プロキシと関連する情報を確認することができます。

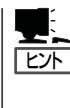
－　FTP情報

[FTP情報]をクリックすると、[プロキシサーバ状態表示(FTP情報)]画面が表示されます。この画面では、FTPプロトコルに関する情報を確認することができます。

Helix Administrator

Helix Universal Server/Helix Universal Proxy(以下Helix)をインストールすると、本システムでストリーミングキャッシュが可能になります。
本システムの管理者はManagement ConsoleからHelix Administrator（HelixのWebベースの管理コンソール）の画面を開き、Helixの設定変更や管理を行うことができます。

Helix Administratorの使用方法

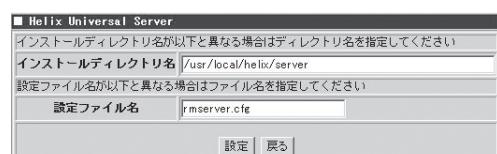
Helix Administratorの呼び出し

3章を参照して指定のディレクトリにインストールを行い、設定ファイル名を変更していない場合は、[開く]をクリックするとHelix Administratorが開き、Helixの設定変更や管理を行うことができます。

[開く]をクリックして新しいウィンドウが開いてもHelix Administratorが表示されない場合は、Helixが起動していない可能性があります。Management Consoleの[システム]画面の[プロセス実行状況]でrmserver(Helix Universal Serverの場合)またはrmproxy(Helix Universal Proxyの場合)が表示されていることを確認してください。

インストール情報の編集

指定のディレクトリ以外の場所にインストールした場合、および設定ファイル名をデフォルトから変更した場合は必ず[編集]をクリックし、インストール情報の変更を行う必要があります。変更を行わなければManagement ConsoleからHelix Administratorの画面を開くことはできません。

- **インストールディレクトリ名**

  Helixをインストールしたディレクトリ名をフルパスで指定してください。

● **設定ファイル名**

設定ファイル名をデフォルトから変更した場合は、そのファイル名を指定してください。

- 3章の「ストリーミングキャッシュソフトウェアのインストール」では以下のディレクトリにインストールすることを推奨しています。

  Helix Universal Server　：/usr/local/helix/server

  Helix Universal Proxy　：/usr/local/helix/proxy

- インストール後に手動で設定ファイル名を変更していない限りは、「設定ファイル名」の項目は修正する必要はありません。

  なお、デフォルトの設定ファイル名は以下のようになっています。

  Helix Universal Server　：rmserver.cfg

  Helix Universal Proxy　：rmproxy.cfg

バックアップ/リストア

システムの故障、設定の誤った変更など思わぬトラブルからスムーズに復旧するために、定期的にシステムのファイルのバックアップをとっておくことを強く推奨します。
バックアップしておいたファイルを「リストア」することによってバックアップを作成した時点の状態へシステムを復元することができるようになります。
本装置では、システム内のファイルを以下の4つのグループに分類して、その各グループごとにファイルのバックアップのとり方を制御することができます。

- システムの設定ファイル
- プロキシサーバの設定ファイル
- 各種ログファイル
- プロキシアクセス統計情報

上記以外のファイルについては[ディレクトリ指定]からバックアップを行うことができます。詳細はオンラインヘルプを参照してください。

初期状態では、いずれのグループも「バックアップしない」設定になっています。お客様の環境にあわせて各グループのファイルのバックアップを設定してください。
本装置では各グループに対して「ローカルディスク」と「Samba」の2種類のバックアップ方法を指定することができます。
各方法には、それぞれ以下のような特徴があります。

- ローカルディスク

  内蔵ハードディスクの別の場所にバックアップをとります。

- Samba

  LANに接続されているWindowsマシンのディスクにバックアップをとります。

重要

- **システムの設定ファイル、およびプロキシサーバの設定ファイルは必ずバックアップを設定してください。**
- **ローカルディスクへのバックアップは、他の方法に比べてリストアできない可能性が高くなります。なるべくSambaを使用して、別マシンへバックアップをとるようにしてください。**
- **Sambaでのバックアップは、内蔵ハードディスクがクラッシュしても復元を行うことができますが、あらかじめ、Windowsマシンに共有の設定をしておく必要がありますので注意してください。**
- **キャッシュサーバアクセスログおよびキャッシュログは、「各種ログファイル」のバックアップでの対象外となりますので、注意してください。**

「Samba」によるバックアップ設定の例

ここでは「Samba」を使用したバックアップの方法について説明します。
例として「workgroup」内に所属するマシン名「winpc」というWindowsマシンの「C:ドライブ」にバックアップのためのフォルダ「cachebackup」を作成して「システムの設定ファイル」グループのファイルのバックアップを行う場合の操作手順を説明します。
バックアップファイルを置くマシン(winpc)でのバックアップ作業のためのユーザーを「winpc」上にあらかじめ用意してください。

重要

バックアップファイルの中にはシステムのセキュリティに関する情報などが含まれるため、バックアップのためのフォルダ(cachebackup)の読み取り、変更の権限などのセキュリティの設定には十分注意してください。(Windows Me/98/95ではセキュリティの設定ができません。そのためお客様の情報が第三者に盗まれる可能性があります。)

バックアップ作業のためのユーザーは既存のユーザーでもかまいませんが、以下の説明では「cacheadmin」というユーザーをあらかじめ用意したという前提で説明します。

次の順序で設定します。以降、順に設定例を説明していきます。

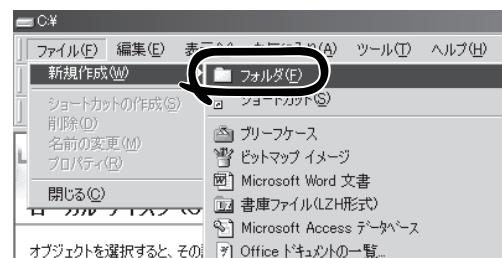
1. Windowsマシンの共有フォルダの作成
2. システムのバックアップファイルグループの設定
3. バックアップの実行

バックアップ用に作成した共有フォルダの設定を不用意に変更するとシステムのバックアップおよび復元の機能が正常に動作しなくなるので注意してください。

Windowsマシンの共有フォルダの作成

まず、バックアップファイルを置いておくための共有フォルダをWindowsマシンに作成します。ここでは、例としてWindows 2000、Windows NT、Windows 98の3種のOSでの作成方法を説明します。

操作例:winpcのOSがWindows 2000の場合

1. マシン「winpc」のデスクトップ上にある[マイコンピュータ]をダブルクリックする。
2. 開いた[マイコンピュータ]ウィンドウの[C:ドライブ]のアイコンをダブルクリックする。
3. [ファイル]メニューの[新規作成]→[フォルダ]をクリックする。

4. [新しいフォルダ]の名前に[cachebackup]とキーボードから入力し<Enter>キーを押す。

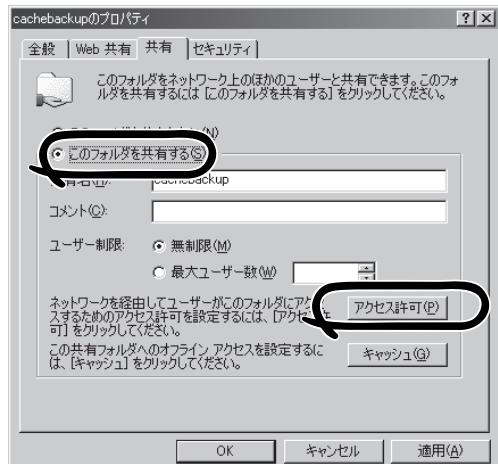
5. 上記の手順で作成した[cachebackup]フォルダをクリックして選択する。

6. [ファイル]メニューの[共有]をクリックする。

   [cachebackupのプロパティ]ウィンドウの[共有]シートが表示されます。

7. [このフォルダを共有する]をクリックする。

8. [アクセス許可]をクリックする。

9. [共有アクセス許可]を設定する。

   ここでは以下のように設定します。

   1. [名前]一覧から[Everyone]を削除する。
   2. [追加]をクリックして[ユーザー、コンピューター、またはグループの選択]ウィンドウでユーザー[cacheadmin]を追加して[OK]をクリックする。
   3. [共有アクセス許可]の[アクセス許可]一覧の[フルコントロール]の許可のチェックボックスにチェックをつける。

10. [OK]をクリックして[cachebackupのアクセス許可]のウィンドウを閉じる。

11. [OK]をクリックして[cachebackupのプロパティ]のウィンドウを閉じる。

12. [cachebackup]フォルダのアイコンが変わったことを確認する。

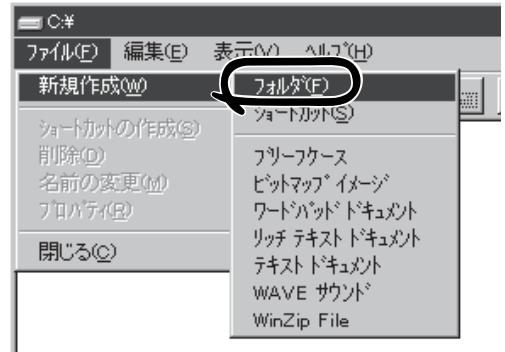
以上でWindows 2000上の共有フォルダの設定は完了です。

操作例：winpcのOSがWindows NTの場合

1. マシン「winpc」のデスクトップ上にある［マイコンピュータ］をダブルクリックする。

2. 開いた［マイコンピュータ］ウィンドウの［C:ドライブ］のアイコンをダブルクリックする。

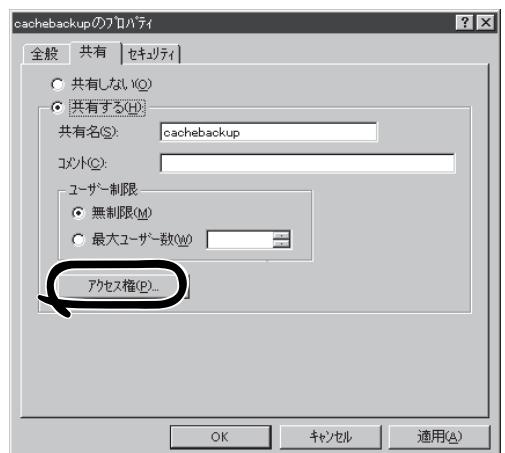
3. ［ファイル］メニューの［新規作成］→［フォルダ］をクリックする。

4. ［新しいフォルダ］の名前に［cachebackup］とキーボードから入力し<Enter>キーを押す。

5. 上記の手順で作成した［cachebackup］フォルダをクリックして選択する。

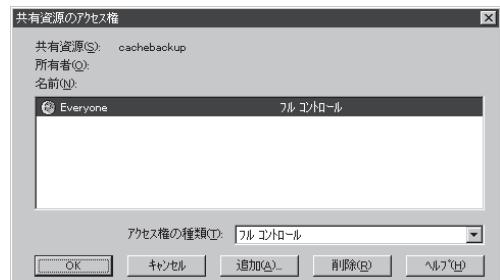
6. ［ファイル］メニューの［共有］をクリックする。

   ［cachebackupのプロパティ］ウィンドウの［共有］シートが表示されます。

7. ［共有する］をクリックする。

8. ［アクセス権］をクリックする。

9. ［共有資源のアクセス権］を設定する。

ここでは以下のように設定します。

1. ［名前］一覧から［Everyone］を削除する。
2. ［追加］をクリックして［ユーザーとグループの追加］ウィンドウで［ユーザーの表示］をクリックしてユーザー［cacheadmin］を選択して［追加］をクリックする。
3. ［アクセス権の種類］のプルダウンメニューから［フルコントロール］を選択して［OK］する。

10. ［OK］をクリックして［共有資源のアクセス権］のウィンドウを閉じる。

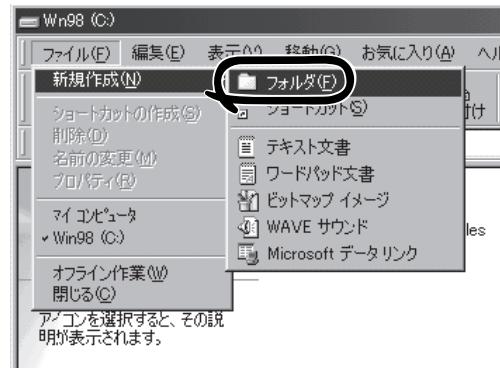
11. ［OK］をクリックして［cachebackupのプロパティ］のウィンドウを閉じる。

以上でWindows NT上の共有フォルダの設定は完了です。

操作例：winpcのOSがWindows 98の場合

1. マシン「winpc」のデスクトップ上にある［マイコンピュータ］をダブルクリックする。

2. 開いた［マイコンピュータ］ウィンドウの［C:ドライブ］のアイコンをダブルクリックする。

3. ［ファイル］メニューの［新規作成］→［フォルダ］をクリックする。

4. ［新しいフォルダ］の名前に［cachebackup］とキーボードから入力し<Enter>キーを押す。

5. 上記の手順で作成した［cachebackup］フォルダをクリックして選択する。

6. ［ファイル］メニューの［共有］をクリックする。

［cachebackupのプロパティ］ウィンドウの［共有］シートが表示されます。

7. ［共有する］をクリックする。

8. ［アクセスの種類］で［フルアクセス］をクリックする。

重要

［パスワード］の［フルアクセス用］欄には何も設定しないでください。

9. ［OK］をクリックして［cachebackupのプロパティ］のウィンドウを閉じる。

以上でWindows 98上の共有フォルダの設定は完了です。

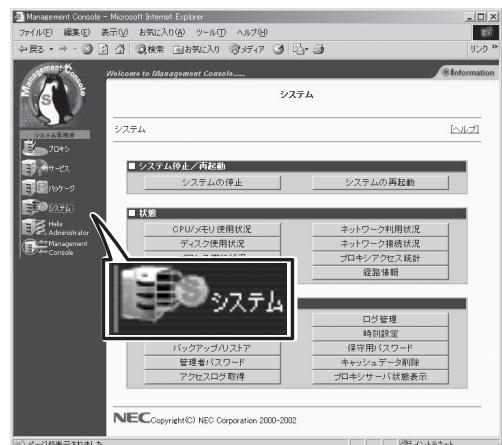
システムのバックアップファイルグループの設定

ここでは例として［システムの設定ファイル］グループのバックアップの設定手順を説明します（他のグループも操作方法は同じです）。

1. Management Console画面左の［システム］アイコンをクリックする。

   ［システム］画面が表示されます。

2. ［システム］画面の［その他］一覧の［バックアップ/リストア］をクリックする。

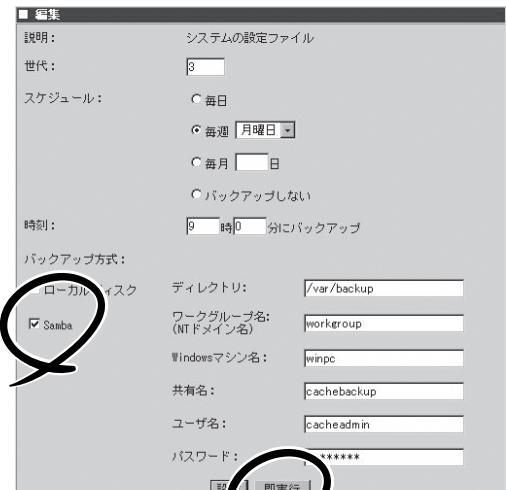
   ［バックアップ/リストア一覧］画面が表示されます。

3. 一覧の［システムの設定ファイル］の左側の［編集］をクリックする。

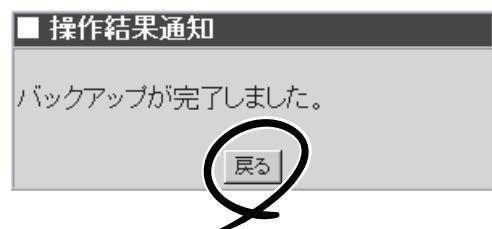
   バックアップ設定の［編集］画面が表示されます。

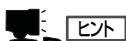
■ バックアップ/リストア一覧

操作	説明	世代数	タイミング
バックアップ 編集 リストア	システムの設定ファイル	5	バックアップしない
バックアップ 編集 リストア	プロキシサーバの設定ファイル	5	バックアップしない
バックアップ 編集 リストア	各種ログファイル	5	バックアップしない
バックアップ 編集 リストア	プロキシアクセス統計情報	5	バックアップしない

4. ［編集］画面のバックアップ方式の［Samba］をクリックして選択する。

5. 「Windowsマシンの共有フォルダの作成」で行った設定に従って以下の項目を入力する。
   - ワークグループ(NTドメイン名):workgroup
   - ［Windowsマシン名］: winpc
   - ［共有名］: cachebackup
   - ［ユーザ名］: cacheadmin
   - ［パスワード］: ユーザcacheadminのパスワード

6. 正しく設定されていることを確認するため［即実行］をクリックしてバックアップを実行する。

   正しく実行された場合は右の操作結果通知が表示されます。

正しく操作結果通知が表示されない場合はWindowsマシンの共有の設定とバックアップ方式の設定が正しいかどうか確認してください。

ヒント

この［即実行］を使うことで、任意のタイミングで手動でバックアップを行うことができます。

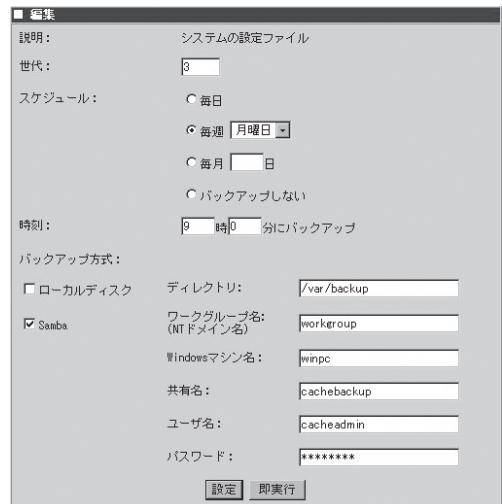
7. ［戻る］をクリックする。

定期的に自動的にバックアップを行うには次の設定を続けて行ってください。

8. [編集]画面で[世代]、[スケジュール]、[時刻]を指定する。

右図の例では[毎週月曜日の朝9:00にバックアップをとる。バックアップファイルは3世代分残す]設定を行う場合を示しています。

世代

バックアップファイルをいくつ残すかを指定します。バックアップファイルを保管するディスクの容量と、必要性に応じて指定してください。世代を1にすると、バックアップを実行するたびに前回のバックアップ内容を上書きすることになります。

スケジュール

バックアップを実行する日を指定します。[毎日]、[毎週]、[毎月]、および[バックアップしない]から選択します。

[毎週]を指定する場合は右側の曜日も選択してください。

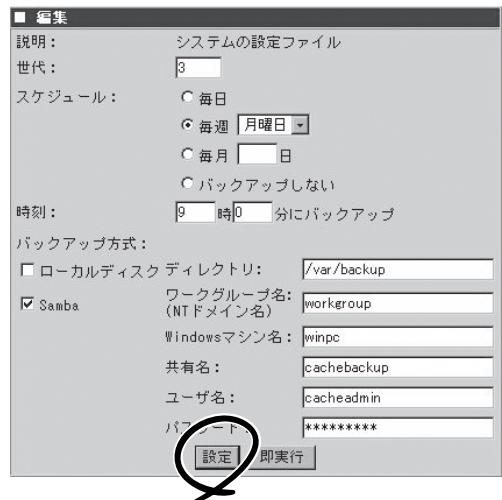
[毎月]を指定する場合は右側のテキストボックスに日付を入力してください

いずれの場合も指定した日付に本体の電源とバックアップ先のマシンの電源が入っていない場合はバックアップできないので注意してください。

時刻

[スケジュール]で指定した日付の何時何分にバックアップを行うかを指定します。指定した時刻に本体の電源とバックアップ先のマシンの電源がONになっていない場合はバックアップできないので注意してください。

9. [編集]画面下の[設定]をクリックする。

以上で、定期的に自動的にバックアップを行う設定は完了です。

バックアップの実行

バックアップの処理は「システムのバックアップファイルグループの設定」で指定した日時に本体の電源とバックアップ先のマシンの電源が入っていない場合は、バックアップされませんので注意してください。

リストア

バックアップファイルは4つの各バックアップファイルグループごとにシステムにリストアすることができます。
ここでは例として[バックアップ手順の例]で設定を行った[システム設定のファイル]グループのファイルのバックアップファイルをシステムにリストアする際の操作手順の例を説明します。

1. Management Console画面左の[システム]アイコンをクリックする。

   [システム]画面が表示されます。

2. [システム]画面の[その他]一覧の[バックアップ/リストア]をクリックする。

   [バックアップ/リストア一覧]画面が表示されます。

3. 一覧の[システムの設定ファイル]の左側の[リストア]をクリックする。

   [リストア]画面が表示されます。

■ バックアップ/リストア一覧

操作	説明	世代数	タイミング
バックアップ 編集 リストア	システムの設定ファイル	5	バックアップしない
バックアップ 編集 リストア	プロキシサーバの設定ファイル	5	バックアップしない
バックアップ 編集 リストア	各種ログファイル	5	バックアップしない
バックアップ 編集 リストア	プロキシアクセス統計情報	5	バックアップしない

4. [リストア]画面で[バックアップのリストア先]、[バックアップ方式]、[リストアするバックアップファイル]を指定し、[リストア]をクリックする。

   通常は、デフォルトで最も新しいバックアップファイルが選択されています。そのまま実行すれば、最新のバックアップファイルがリストアされます。

   重要

   [元のディレクトリにリストアする]を選択した場合、現在のファイルの内容がバックアップしておいた内容で上書きされますので注意してください。

5. 「リストアします。よろしいですか？」というダイアログボックスが表示されます。リストアする場合は[OK]をクリックする。

   リストアをしない場合は、[キャンセル]をクリックしてください。

   ヒント

   選択したバックアップファイルの内容を参照したい場合は、[表示]をクリックしてください。